NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A PROACTIVE STRATEGY TOWARD TERRORISM AND TRANSNATIONAL CRIME

by

John R. Hoyt

December 1998

Thesis Advisor: John Arquilla

Approved for public release; distribution is unlimited.

QUALITY INSPECTED 4

19990219090

Preceding Pages Blank

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of informationSend comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1998	Master's Thesis

4. TITLE AND SUBTITLE: A PROACTIVE STRATEGY TOWARD TERRORISM AND TRANSNATIONAL CRIME

5. FUNDING NUMBERS

6. AUTHOR(S)
John R. Hoyt

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(maximum 200 words)***

Terrorist and transnational criminal organizations are evolving into enormous national security threats. Their embrace of advanced information and communications systems has significantly enhanced their organizational efficiency as well as provided them with an exceptional disruption weapons system. The US's heavy reliance upon the information infrastructure, along with the disruptive and destructive capabilities of cyberterror and cybercrime, have created a potentially very dangerous situation. In addition, the proliferation of advanced weapons systems into terrorist hands, including WMDs, requires the US to reassess its counter-terror and crime policy. The current strategy in place to combat these entities is lacking, as can be seen by the World Trade Center and Oklahoma City bombings. The employment of an aggressive, proactive strategy that focuses on information operations is necessary to constrain these growing threats. The proactive strategy is accompanied by new significant costs. However, when compared to the cost of current US strategy, proactive measures are seen to provide enormous overall savings. The proactive strategy is comprised of three elements: intelligence collection, disruption and destruction. Today's advanced technologies provide the US with the tools and weapons necessary to engage in and win the war against terror and crime.

14. SUBJECT TERMS
Terror, Transnational Crime, Information Operations,

15. NUMBER OF PAGES
120

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

A PROACTIVE STRATEGY TOWARD TERRORISM AND TRANSNATIONAL CRIME

John R. Hoyt
Lieutenant, United States Navy
B.S., United States Naval Academy, 1989

Submitted in partial fulfillment of the
Requirements for the degree of

MASTERS OF SCIENCE IN DEFENSE ANALYSIS (FINANCIAL MANAGEMENT)

from the

NAVAL POSTGRADUATE SCHOOL
December 1998

Author: _____
John R. Hoyt

Approved by: _____
John Arquilla, Thesis Advisor

_____
David Tucker, Second Reader

_____
Maurice D. Weir, Chairman
Special Operations Curriculum Committee

ABSTRACT

Terrorist and transnational criminal organizations are evolving into enormous national security threats. Their embrace of advanced information and communications systems has significantly enhanced their organizational efficiency as well as provided them with an exceptional disruption weapons system. The US's heavy reliance upon the information infrastructure, along with the disruptive and destructive capabilities of cyberterror and cybercrime, have created a potentially very dangerous situation. In addition, the proliferation of advanced weapons systems into terrorist hands, including WMDs, requires the US to reassess its counter-terror and crime policy. The current strategy in place to combat these entities is lacking, as can be seen by the World Trade Center and Oklahoma City bombings. The employment of an aggressive, proactive strategy that focuses on information operations is necessary to constrain these growing threats. The proactive strategy is accompanied by new significant costs. However, when compared to the cost of current US strategy, proactive measures are seen to provide enormous overall savings. The proactive strategy is comprised of three elements: intelligence collection, disruption and destruction. Today's advanced technologies provide the US with the tools and weapons necessary to engage in and win the war against terror and crime.

TABLE OF CONTENTS

I. INTRODUCTION

Current US security policy indicates an overwhelming belief in an established state of peace and the confidence that our armed forces can adequately respond to all emerging threats. The Department of Defense budget has seen a drastic reduction from an all time high of 338.3 billion dollars in 1989 to 237.4 billion in 1997, (in constant 1987 dollars). In addition, force manning levels have dropped from 2.13million active duty personnel in 1989 to 1.47 million in 1996.[1]

US security strategy consists of three key elements; Shape, Respond and Prepare.[2] These elements support the belief in a current state of peace and lack of significant threat. To expand this point further, The Joint Chiefs of Staff have stated that our military objectives are to "promote peace and stability and when necessary, to defeat adversaries." The term "when necessary" implies that US policy makers currently see no legitimate and active threat to US security.

The most significant event to inspire this belief and one that promoted a shift in the national security policy occurred in 1991. The dissolution of the Soviet Union eliminated the only true viable contender to US warmaking capability. This left the United States possessing the most dominant military force in the world. The removal of Soviet troops from Eastern Europe has averted what was once believed to be an inevitable major armed conflict in the European theater. Since these dramatic events, the potential for a conflict involving significant US conventional forces or the use of nuclear

[1] Taken from US Department of Commerce, 117 edition, Economics & Statistics administration.

weapons has become remote. As Russia struggles with the transformation to a democratic system, the potential exists for the return of the "evil empire." However, the threat of war remains low due to Russia's massive domestic problems and significant deterioration in its military readiness and weapons systems. Perhaps the largest immediate concern to US national security is the potential proliferation of Soviet nuclear material.

While the number of countries that possess nuclear arms is increasing in number, the threat posed by states actually using these weapons is minimal.[3] The threat that a state will use these weapons against the US is even more unlikely due to most countries lack of delivery technology and fear of US massive retaliation. As seen recently with both India and Pakistan, possession of these weapons is more of a cry for recognition than a legitimate threat of use.

China, arguably US's next great power rival, is still estimated to be many years away from obtaining a military level adequate to confront US forces. In addition, analysis of China's foreign policy objectives indicates no apparent ill-intentions to US interests. The area that currently demands greatest US attention is the Korean Peninsula. While N. Korea possesses a large conventional force, the maintenance and operational efficiency of the equipment and personnel are estimated to be very poor. Even the use of nuclear weapons, in a "conventional" manner, would not significantly enhance N. Korea's military and political position against the vastly superior combined ROK and US coalition.

---

[2] National Military Strategy, *Shape, Respond, Prepare now- A Military Strategy for a New Era,* CJCS, 1997

[3] This argument is presented in Martin Van Creveld, *The Transformation of War,*(New York: The Free Press, 1991), pp. 2-10

On the conventional battlefield, the United States maintains an overwhelming superiority in military capability. The conduct of Operation Desert Storm exemplified the relative ease with which US military forces were able to defeat a significantly large army. While the quality of Iraqi forces was clearly suspect, they were overwhelmingly the dominant regional military force. US commitment to maintain its high quality force, the continued research and development of communications and intelligence technologies and a strong economic base will ensure that this conventional military dominance continues. As stated in the national military strategy;

> "Given the United States' military potential and ability to deploy to any region of conflict, it is unlikely that any regional power or coalition could amass sufficient conventional strength to defeat our Armed Forces."[4]

The introduction and application of systems like "land warrior" and "applique" and ever evolving smart and "brilliant" weapons systems will continue to enhance US warfighting capabilities and widen the gap between future competitors. In addition, the revamping of US doctrine which include concepts like "Total Spectrum Dominance" and "C4I for the Warrior" are part of a continued effort to ensure this dominance through ongoing capabilities and requirements analysis.

However, this confidence in the US military's ability to insulate the US from overt threat is an illusion created by an exclusive focus on state actors. When the threat from non-state actors is considered, this comfort zone quickly erodes. The potential for terrorist activity against American targets, both domestically and overseas, is an omnipresent threat that the US has never fully comprehended. While both the national

[4] National Military Strategy, 1997

and military security strategies acknowledge this threat, they provide little in terms of response, except to say:

> "We must increase our capabilities to counter these threats and adapt our military doctrine, training and equipment to ensure a rapid and effective joint and interagency response."[5]

Historically, terrorist activity within the confines of the United States itself has been relatively minute in both quantity and quality. These events have been relegated to relatively inept and ineffective organizations like the "weathermen" and the Puerto Rican based FLN. Thus, terrorism is not viewed as a major concern by the majority of the American public. This lack of public concern has made terrorism a relatively minor political issue, placing it near the bottom of the list of many politicians that need more "relevant" issues to get reelected.

Recent events, including the Oklahoma city and the New York World Trade Center bombings, have hinted at the incredible vulnerabilities within the United States. These attacks, along with the increased publicity given to domestic militant organizations, have had only a modest sobering effect. In addition to the increased domestic threat, US continued involvement in world affairs will inevitably raise the animosities of some foreign state or non-state actors. The frustration over US "meddling," along with the inability to confront the US on the conventional battlefield, may compel them toward unconventional measures. This asymmetric method of warfare may include the use of terrorist tactics.

The increased capabilities and diverse nature of terrorist organizations will increasingly present a serious threat to US interests abroad and within the US.[6] Terrorists

have recently displayed an increased willingness to use more powerful explosives, including use of chemical and biological agents.[7] This trend, along with the very real threat of nuclear proliferation into terrorist hands, presents the US with an unexpectedly high cost of continued neglect of this issue.

While the thought of terrorist use of a nuclear device is sobering, a relatively new and vulnerable target has arisen: America's advanced computer-based infrastructure. The United States' ever increasing reliance upon information-based systems, in virtually every aspect of life, makes an exceptionally rich target for terrorist acts of disruption. The advent of cyberterror poses a real and significant threat to the US.[8] The Internet connects virtually all aspects of government, commerce and individual lives around the world. While this process has significantly increased efficiency, speed and availability of information, it also allows access by unauthorized and ill-intentioned persons. The incredible power of personal home computers has opened the realm of computer warfare to virtually every individual that can afford a computer, a power outlet, and a phoneline. While the realm of traditional terrorist attacks was limited by both the expense of equipment and the moral dilemma of violence, the cyber terrorist has neither constraint. Disruptive terrorist attacks, because of their lack of lethality, are seen by some as morally more acceptable to both terrorist as well as the constituencies from which they desire acceptance and support.

---

[5] National Military Strategy, 1997

[6] The threat of modern terrorism is presented by Benjamin Netanyahu, *Fighting Terrorism,*(New York: Farrar Straus Giroux, 1995)

[7] John Deutch, "Terrorism: Think Again," *Foreign Policy,* March 1997

[8] The concepts of cyberterror are well presented by Bruce Hoffman in "Responding to Terrorism Across the Technological Spectrum," *Terrorism and Political Violence,* Vol. 6, No. 3, Autumn 1994

Traditional US responses, when confronted with cyberterror, will be seriously challenged and must be reevaluated under such non-lethal yet exceptionally disruptive attacks. While Russia has proclaimed its right to respond to cyberterror with nuclear weapons[9], the US has not yet sufficiently addressed this issue.

The prospect of cyberterror also provides the terrorist with increased anonymity. Traditionally, terrorists wanted publicity to gain recognition for their cause. Today's terrorist may have no such desires. Terrorism as a form of retribution or as an asymmetric method of warfare is both harder to combat and typically more violent. Cyberterror's relative ease of entry, anonymity, and disruptive capability makes this threat potentially more dangerous than conventional terrorist acts of destruction.

In addition to the increased threat of terrorism, the dissolution of the Soviet Union has opened the floodgates for transnational criminal organizations. Once kept in check by hard-line Soviet intelligence and police agencies, many new and ethnically oriented criminal enterprises have emerged within the former Soviet Union. These Russian organizations along with the Chinese Triads and Japanese Yakuza (to name only two), have brought about an unprecedented level of world crime. Displaying exceptional willingness to cooperate, these organizations have established ties amongst themselves and the more established Colombian drug cartels and Sicilian Mafia. These relationships have proven extremely beneficial, opening new drug distribution areas, while breathing new life into declining organizations.

Taking advantage of unstable and weak governments, these criminal organizations have been able to flourish. In many cases these groups are able to dictate state action

[9] Timothy L. Thomas, "The Threat of Information Operations: A Russian Perspective," Pfaltzgraff, *op cit*

through corruption, bribes, threats and outright murder. This is best exemplified in Colombia, in which the level of corruption has reached incredible proportions and has undermined the ability of the official government to function appropriately. This influence over government action is not only detrimental to a state's ability to preside within its own territory, but affects the state's foreign policy as well. This can lead to decreased cooperation with US law enforcement efforts, and conflicts in immigration, customs, trade, and basic international relations.[10] The continued and virtually unchecked assault from these criminal organizations constitutes a direct attack upon US society itself. The blatant disregard for US law has and will continue to result in lives lost, billions of dollars in lost revenue, violent crime and a general destabilization of US society. The United States must treat this assault as an act of war and take appropriate measures to reverse the process which is progressively deteriorating the established society and security of the nation.

Similar to terrorists, TCOs are taking full advantage of the information revolution, and have subsequently become significantly more organized and efficient. The technological capabilities and personnel discipline exercised by these groups is exceptional. Many have enlisted the help of professionals in the business, intelligence and communications realms. As these organizations continue to expand they become increasingly more reliant upon advanced technologies to organize and maintain their "business" affairs. Among the greatest utilities of these systems is their ability to transfer and launder huge amounts of "dirty" money around the world. In addition, computers

[10] A good discussion on the threats of transnational criminals is provided by Phil Williams, "Transnational Criminal Organizations and National Security," *Survival,* Vol. 36, No. 1, Spring 1994, pp. 96-113

have been used to perform advanced criminal business schemes. As FBI director Louis Freeh stated;

> "It is a much more sophisticated type of organized crime than we have ever seen in the United States. It goes to Cybercrime. It goes to complex fraud schemes. It goes to money laundering schemes and operations which involve hundreds of millions of dollars."[11]

The nature of both terrorists and criminals predisposes them toward forming relationships with each other. Terrorist organizations require significant funding in order to function effectively. While some of this funding is gained through individual and state sponsorship, an increased trend toward the conduct of illegal activity has occurred. The money, acquired primarily through drug trafficking, is utilized to bankroll terrorist activities and purchase state-of-the-art weaponry. In addition, criminal organizations have increasingly relied upon violent, terrorist-like attacks to intimidate or eliminate potential opposition. These attacks include activities against competitors, as well as law enforcement and governmental agencies. The trend of increased cooperation and the melting of roles between terrorist and criminal has produced a significantly more diverse, complex, capable and agile threat.

The strategy currently in place for combating both terrorism and crime is comprised of three elements: prosecution, prevention and no concessions.[12] These tactics have created a US policy that, with limited exceptions, is reactive in nature. US counter-crime and terrorist efforts go into full swing only after a crime or terrorist act has been

[11] From testimony of FBI director Louis Freeh before the House of Representatives, Committee on International Relations, Oct 1,1997

[12] Taken from GAO report "Combating Terrorism," Sep 1997

committed. The attacks at the Oklahoma federal building as well as the New York World Trade Center are two clear examples in which the current US policy proved inadequate.. With regard to crime, the US has performed equally poorly, as evidenced by the Colombian cartel's booming $5 billion narcotics trade. As former secretary of state George Shultz said in 1984, "a purely passive defense does not provide enough of a deterrent to terrorism and the states that sponsor it."[13]

In order to address these growing crises, the US must implement an aggressive, proactive strategy that carries the fight to the terrorists and criminals. The advance in information and communications systems provides the US with the tools and weapons necessary to carry this out. The conduct of Information Operations (IO) provides and exceptionally diverse and flexible capability that can be tailored to meet the characteristics of virtually any target. Within the proposed proactive strategy, IO is separated into two tactics: preemption and destruction. Preemption is conducted as a means of striking a target in expectation of being struck and acting to head off the attacker prior to his ability to act. The disruptive tactic goes to the roots of terror and crime, attacking the terrorist or criminal organizations simply because they are terrorists or criminals. The proactive strategy will place these organizations on the defensive, hampering their ability to perform future operations.

However, the increased proficiency of an IO-based proactive strategy is accompanied by new significant costs. In order to justify strategy implementation, these costs must be analyzed and compared to the costs incurred under the current reactive strategy. Analyzing the costs associated with terrorism and crime reveals seven major

[13] Patrick Pexton, "Cohen Focuses Sights on Terrorism," *Navy Times,* Sep 22, 1997

cost factors: human lives, material damage, reputation, precedent, escalation, foreign sovereignty, and civil liberties. These costs must be valued, not just in monetary terms, but in terms of their relative importance in maintaining American society.

In order to implement this proactive strategy, US intelligence and federal law enforcement agencies must undergo a significant paradigm shift. In addition, politicians must be willing to withstand the public's expected outcry on any movement that would erode civil liberties in any way, while increasing law enforcement authority. Leaving the policy the way it presently is invites disaster. The government is currently ill-organized to combat crime and terror. Perhaps the most telling aspect of this inefficiency is seen within the organizational quagmire that the US government has established in an effort to combat terrorism. With each agency closely guarding their "turf," the resulting structure is confusing and disconcerted.

The drastic change seen within the terrorist and criminal organizations requires more than just the semantic changes in policy that have occurred since the 1970s. These phenomena are becoming increasingly dangerous. Their growth, abilities and destructive force must place them on the top of US national security issues. Adopting a proactive strategy that incorporates IO is required in order to jar terrorists and transnational criminals from their current comfort zone.

The following analysis is performed in four sections. Chapter II examines the emerging trends and capabilities of terrorist and criminal organizations. Chapter III takes a look at the current US reactive strategy and compares it to the proposed proactive one. Chapter IV analyzes the cost factors associated with both strategies and compares the

"aggregate costs." Chapter V discusses the evolving advanced capabilities within an IO-based strategy.

II. OLD THREATS, NEW FACES

Both terrorism and crime have been a part of human society since the beginning of time. Some terrorist acts have had repercussions beyond the immediate geographic region in which they were committed, as exemplified by the assassination of the Archduke Franz Ferdinand, which started World War I. However, these acts have predominantly been a local and internal concern. Then, in 1972, a Palestinian terrorist attack on the Israeli Olympic team in Munich Germany ushered in what is called by many as the modern age of terrorism.[14] This attack displayed terrorists' increased willingness to ignore international boundaries, and to strike anywhere in the world. In the criminal realm, organizations grew in significance in US society in the 1920s, with the formation of the first national crime syndicate. This arrangement effectively linked all Mafia crime families across the country, creating a powerful and diverse threat to US society. Today's advanced information and communications technologies have energized the evolution of both terror and crime to new, higher levels of concern. The threats now posed by information-savvy terrorists and criminals are virtually boundless, in both the geographic and destructive sense. These "global" non-state actors currently present the US with perhaps the greatest threat to national security. Unlike North Korea or Iraq, which pose the potential for war, terrorists and criminals are actively and continuously engaging in a kind of warfare.

[14] John Deutch, "Terrorism: Think Again," *Foreign Policy*, Summer 1997

One of the greatest barriers to understanding the magnitude of this threat is the lack of a mutually acceptable definition of terrorism[15]. Not only does the definition of terrorism vary between countries, which many times employ a label in order to justify their actions, but federal agencies within the US itself are unable to formulate a consensus on what does or does not constitute a terrorist act. While government agencies spend considerable time and effort propounding their favored definitions, in an attempt to justify continued operating budgets, the terrorists and criminals continue to extend their operations at a staggering pace. In addition, criminal organizations' growing reliance on terrorist-type acts has exacerbated the problem.[16] Rather than attempt to modernize the definition of terrorism, this chapter will examine the predominant characteristics of these modern non-state actors in order to provide an accurate assessment of the threat they pose to US national security. The characteristics that will be analyzed are their motives, professional status, sphere of influence, organizational structure and operational tactics.

A. MOTIVATION

One of the keys to developing a proper counter strategy to both terrorism and crime is gaining a clear understanding of the motivations behind their existence.[17] Terrorism has long been believed to be purely politically motivated. In fact, the majority of definitions have incorporated this notion into their description of terrorism. For

[15] The difficulties in determining an acceptable definition of terrorism is discussed in Brian Jenkins, "The Study of Terrorism: Definitional Problems," *Behavioral and Quantitative Perspectives on Terrorism,* edited by Yonah Alexander and John M. Gleason, 1978

[16] This blurring is discussed by Walter Laqueur, "Postmodern Terrorism," *Foreign Affairs,* September/October 1996 as well as in Senator John Kerry's book *The New War,(New York:* Simon & Shuster, 1997)

example, both the US Department of State and Defense both currently define terrorism as premeditated, politically motivated violence. While this belief may have held true for the majority of terrorist attacks in the 1970s, today's terrorists may have few specific political aspirations. Even an act initially viewed as political may prove to hold other underlying motives when more closely examined. Thus, a blurring of motivations is increasingly observed among these non-state entities. This is best exemplified by the numerous Colombian political assassinations that are performed in an effort to secure or enhance the drug cartel's prosperity[18]. While there are seemingly an unlimited number of motives behind the conduct of terrorist or criminal acts, the more significant threats can be categorized into one of three headings: political, religious, and monetary[19].

The political actor is perhaps the most familiar. The politically motivated terrorist attempts to bring about a change in the political system by use of coercive violent action[20]. These groups resort to terrorism because they are unable to effect a change through the legitimate state or international system. Thus political terrorism has been described as a tool for the weak. This description applies equally to a minority group (in terms of influence, not necessarily numbers) within a state system or a state within the international system.

---

[17] This shift in terrorist motives is discussed in Roger Medd & Frank Goldstein, "International Terrorism on the Eve of a New Millennium," *Studies in Conflict & Terrorism,* 20:281-316, 1997

[18] Since 1989, Colombia has lost four presidential candidates, more than sixty judges, more than seventy journalists and more than 1000 police officers, John Coleman, "Statement of the Assistant Administrator for Operations of the Drug Enforcement Administration Before the U.S. Senate Subcommittee on Terrorism, Narcotics, and International Operations of the Committee on Foreign Relations," in *Recent Developments in Transnational Crime Affecting U.S. Law Enforcement and Foreign Policy; Mutual Legal Assistance Treaty in Criminal Matters With Panama, Treaty Doc. 102-15*

[19] Medd & Goldstein, "International terrorism on the eve of a new millenium," describe the three motivations as political, religious and economic, p. 282

[20] An excellent discussion of "domestic" political terrorism is provided in Thomas Thornton, "Terror as a Weapon of Political Agitation," *Internal War,* edited by Harry Eckstein, (West Port: Greenwood Press, 1964)

The politically motivated terrorist will normally aspire to one of four objectives. The terrorists may desire to influence a change on a particular government issue. This can be seen in the recent terrorist attacks in Israel which were intended to derail the Oct 98 peace agreements with the Palestinians. The terrorists may desire a complete change in state leadership. This goal was exemplified by the assassination of US President McKinley[21]. The terrorist group may desire a complete separation from the existing state control system as is observed with the IRA's struggle with Britain. The last objective is to advance the political objective of a sponsor state. This last objective demonstrates terrorist employment as a form of warfare by a foreign government that is itself too weak to institute a change in the international system by means of direct force.

One of the more dramatic developments in the realm of non-state actors is the rise of religious-based violence. While religion has played a role in many past cases,[22] the resurgence of Islamic Fundamentalism has driven it to the forefront of terrorism today. Perhaps the largest catalyst to this religious-based terrorism was the rise of Ayatollah Khomeini in Iran.[23] While he cannot be held solely accountable for this upsurge, he was arguably the most influential factor in its rise. This religious motivation is extremely strong. Where the politically motivated terrorist believes that the current system is flawed or unjust, the religiously motivated terrorist believes that he has been ordained by a

[21] President Mckinley was assassinated by an anarchist named Leon Czolgosz, who desired to bring attention to the anarchist cause and upset the established order.

[22] David C. Rapoport discusses the ancient lineage of terrorism in his analysis of the Thugs, Assassins and the Zealots-Scarii, "Fear and Trembling: Terrorism in Three Religious Traditions," *The American Political Science Review,* Vol. 78 No. 3, September, 1984. pp. 658-677

[23] In 1979 Khomeini declared "Islam is the religion of militant individuals who are committed to the truth and justice. It is the religion of those who desire freedom and independence. It is the school of those who struggle against imperialism. Weapons in our hands are used to realize divine and Islamic aspirations." Robin Wright, *Sacred Rage,* (New York: Simon & Shuster, 1986), p. 27

divine entity to purify the world. This total commitment creates a significantly more dangerous threat. Bruce Hoffman writes that;

> "Whereas secular terrorists generally consider indiscriminate violence immoral and counter productive, religious terrorists regard such violence as both morally justified and a necessary expedient for the attainment of their goals."[24]

In many cases, the religiously motivated terrorist believes that only by purging the world of the "infidels" will he fulfill "God's Will." This belief can easily lead to the use of extremely powerful weapons of destruction. To make matters worse, these individuals have become convinced that, by dying as a martyr, they will receive great rewards in the afterlife.[25] These beliefs render many immune to the fear of dying for the "cause" and their God. Unfortunately for the US, this "cause" often includes the destruction of the American non-believers and the land of the "Great Satan."

The final motivation behind terrorist and criminal acts is money. While crime has been a concern in virtually every nation (even Singapore), the advent of the information age has made it a significant world epidemic. Terrorists and criminals possess this monetary motivation in the ultimate pursuit of one of two goals. The first is simply to become rich and the second is to obtain wealth to purchase equipment and fund further operations. This second goal is seen within many terrorist organizations that do not

---

[24] Bruce Hoffman, "Responding to Terrorism Across the Technological Spectrum," *Terrorism and Political Violence,* Vol 6, No. 3, Autumn 1994, p. 346

[25] "A martyr has six privileges with God: he is forgiven his sins, he is shown a place in paradise he is redeemed from the torments of the grave, he is made secure from the fear of hell, and a crown of glory is placed on his head of which one ruby is worth more than the world and all that is in it, he will marry 72 of the Huris with black eyes, and his intercession will be accepted for 70 of his kinsmen." David Rapoport, "Sacred Terror: A Contemporary Example from Islam," *Origins of Terrorism: Psychologies, Theologies, State of Mind,* ed. Walter Reich, (New York: Woodrow Wilson International Center for Scholars and Cambridge University Press, 1990), pp. 117-118

possess adequate monetary support from either state or non-state sponsors. It is primarily within the realm of monetary motivation that the distinctions between terrorist and criminal organizations blur, as is exemplified by the numerous kidnappings performed in Latin America.[26] Where the ultimate goal of these acts may have originally been political, the acquisition of money has become their primary focus. While the terrorists believe these acts are simply a means to an end, the accumulation of wealth can easily become an end unto itself.

B. SPHERE OF INFLUENCE

As mentioned in the beginning of the chapter, terrorism has evolved from an internal or domestic concern into an international dilemma. The eager acceptance of the information age by both terrorists and criminals has drastically expanded both the geographic scope and capabilities of their operations. Yet, while intelligence and communications technologies are now available to virtually every potential criminal or terrorist, not all will take advantage of the increased opportunities. The degree to which these organizations can benefit from the employment of advanced technologies is determined, in part, by their geographic area of concern.

Traditional domestic terrorists play by slightly different rules than their international counterparts. While domestic terrorists may find it necessary to perform operations outside of their immediate territory, the act is intended to influence local government and constituency. Thus in many cases they must limit their destructive

[26] "In Colombia someone is kidnapped every six hours. In Rio de Janeiro someone is kidnapped every four days. Brian Jenkins counted a total of 6,000 kidnappings in Latin America in 1994." Medd & Goldstein, p.

desires in order to prevent complete alienation.[27] In their effort to gain public support, domestic terrorists must be seen to possess ability and strength. Thus, many of the domestic incidents, at least the politically motivated ones, are high profile events that cause minimal death and destruction.

Timothy McVeigh, the convicted perpetrator of the Oklahoma City bombing, displays a second, potentially more dangerous, type of domestic terrorism. This type of terrorist conducts operations as a symbolic act, with only very broad, indefinite goals in mind. Many times this goal is simply to demonstrate disgust and disdain for the current system. These domestic terrorists will normally be of amateur status, as discussed below, and will be either loners or associated with a very small number of colleagues. Because these domestic terrorists do not strive to gain public support, their destructive desires are no longer limited. Thus this type of domestic terrorist feels that the greater the destruction, the greater the victory and the louder the cry of disapproval. This type of domestic terrorism is also exemplified by the Japanese Aum Shin-Rikyo cult, which perpetrated the sarin nerve gas attack on the Tokyo subway system.

Because these domestic groups have geographically limited goals the logistics necessary to conduct operations are often less stringent than for international terrorists. Perhaps the greatest logistical difference is the monetary requirement. The domestic terrorist may not require extensive travel arrangements, or the establishment of "safe houses," which demand significant money and advanced planning. Working within the confines of native territory allows the domestic terrorist to blend into the population, thus facilitating movement while averting suspicion. "Home field advantage" also precludes

---

285

the need for a great deal of complex administrative planning which includes the difficulties in obtaining weapons and transportation, as well as the minor detail of assembling the operators.

In contrast to the domestic terrorist, the international actor is not directly focused on an internal struggle, but is, in effect, conducting a war against his foreign enemies. Also, in many cases, international terrorist acts are conducted in the interest of a third-party sponsor, and are intended to advance the goals of a particular state. The CIA has attempted to differentiate between a state-sponsored terrorist and an autonomous actor. The CIA defines a terrorist sponsored by a foreign state as international, and the autonomous terrorist as transnational. These definitions are inadequate, due to the terrorists' ability, and desire, to shift from one definition to the other whenever it suits their needs.

The ultimate targets of international terrorists are often the politicians of foreign states, and the international community as a whole. Many times, terrorists have attempted to influence these policy makers by directly attacking the civilian population of that state. This tactic was clearly seen with the World Trade Center bombing, in which the perpetrators were later associated with the Bin Laden terrorist network. Bin Laden's embrace of terrorism is an attempt to influence US policy toward the Arab world.

The destructive potential of international terrorism is significantly greater than that of the domestic terrorist. The indifference to, or even desire for, substantial casualties, and the probable applause rather than alienation from the terrorist's

[27] This concept of the necessity of maintaining popular support is discussed in Martha Crenshaw, "How Terrorism Declines," *Terrorism and Political Violence,* Spring 1991, Vol. 3, No. 1 p. 80

constituency and state sponsor, makes the international terrorist an extremely deadly threat.

The international terrorist requires significant logistical support to carry out attacks, and a sizable monetary "buy in" requirement is a normal characteristic. This money is essential for the proper establishment of an operating base within a foreign state. This entails lodging, the purchase or smuggling of weapons, the potential requirement for falsified documents, and many other items. This monetary requirement can be alleviated through the support of a state or an independent sponsor. However, transferring funds may leave a "footprint" that can be traced to the originator. Thus the logistical requirements, as well as the ability to obtain funding, is considerably more difficult than with the domestic actor. In addition, the international terrorist finds himself operating in an unknown, and often times, hostile environment. While this creates an additional difficulty, the US's commitment to individual rights, regardless of nationality and background, alleviates much of this concern and actually facilitates the activities of the international terrorist.

Transnational criminal organizations, by their very title, are international entities. While these organizations can be broken into their domestic and overseas components, the conduct of operations tends to support a single goal: to generate wealth. Because TCO goals are primarily monetary, they care little about their popularity. As is seen vividly in Russia and Colombia, criminal organizations utilize intimidation, bribery and violence to ensure that the domestic populace remains favorable to their operations. By expending only a fraction of one percent of the profits on administration and support,

these criminal organizations are easily able to meet their logistical requirements, both domestically and overseas.

C. PROFESSIONAL STATUS

One of the emerging trends of terrorist activity today is the shift toward amateurization.[28] While the Hollywood-envisioned "professional" remains a great concern, an increase in "part-time" terrorism has been observed. Amateur terrorists possess numerous distinct characteristics that separate them from their professional counterparts. In many cases, they lack any clearly defined command and control structure, and operations are approved on a consensus basis. The connections between sponsors, either state or otherwise, are also noticeably absent. The size of the amateur organization is inherently very small, and is initially formed through an attraction to or common belief in an ideal, concern or religion. The advent of the Internet has accelerated this pattern. Being able to contact and communicate with others of like attitude, with virtually assured privacy, allows individuals like "white supremacists" to organize. Another common meeting place is religious worship areas. These individuals take full advantage of the Bill of Rights and exercise their right to congregate without fear of intrusion or surveillance. Many of these places of worship, while otherwise fully legitimate, allow extremists to view their opinions, gain support and solicit participants. They further provide a place to plan and stage operations, all under to guise of freedom of religion (e.g., the "Christian Identity Movement").

[28] The concept of amateurization is provided by Bruce Hoffman, "Responding to Terrorism Across the Technological Spectrum," *Terrorism and Political Violence,* Vol. 6 No. 3, Autumn 1994

The ability of police to combat these threats is limited. The group's violent tendencies are normally unknown until after they have committed a terrorist act. Unlike professional terrorists, who have a history of utilizing high technology military equipment, the amateur utilizes over-the-counter material. Thus the tactic of tracing weapons and equipment becomes exceedingly difficult. In addition, the amateur groups may only form for the conduct of a single terrorist attack, then melt back into everyday life after its completion. This hampers the ability to form a profile on these groups, and thus analyze past operations in an attempt to determine future action.

The accessibility of computer technology and the interconnectivity afforded by the World Wide Web provide the amateur terrorist with an exceptionally target rich environment. While labeling a computer hacker a "terrorist" may incite an argument, there is no denying the damage that these individuals can produce. Regardless of motivation, these hackers must be viewed as a legitimate threat that has the potential to warrant national attention.[29]

While the amateur terrorist presents the US with a relatively new and alarming threat, the professional terrorist remains the center of US attention. With the advent of the information age, the professional terrorist is a more elusive, sophisticated and, consequently, dangerous threat. The professional terrorist organization is historically characterized by its well defined command and control structure, training, and "full-time" commitment to the "job". While amateurs may come together to conduct a single act, professionals continuously plan operations and ensure the administrative logistics behind their survival. Some of these professional organizations, in particular the PLO, have extended their operations to include legitimate business practices that ensure their

continued monetary support. This monetary support allows access to state-of-the-art weapons and information systems. The full time employment allows the professional terrorist to fully analyze and observe potential targets. This analysis creates lucrative and productive targets, while significantly increasing the probability of success and escape. While the police and intelligence agencies know of the existence of the larger terrorist organizations, the terrorists themselves are becoming increasingly sophisticated in concealing their operations.

Another disheartening aspect of professional terrorism is the growing cooperation that has been observed in their dealings with criminal organizations. This cooperation provides the terrorists with increased weapons technology, large monetary resources and, most threatening of all, the potential access to nuclear material.[30] As mentioned above, the motivations of these groups are increasingly becoming blurred. As terrorists accelerate their cooperation with criminal organizations, the threat to US security will increase exponentially.

D. ORGANIZATIONAL STRUCTURE

The significant advances in information and communications technologies have drastically altered the organizational structure of legitimate business entities as well as ill-intentioned non-state actors.[31] As information systems continue to evolve, many terrorists and criminals will adapt their organizational structures to take full advantage of these

[29] #3 threat in current national security strategy

[30] For example, the Russian Mafia has expressed its desire to sell stolen Soviet nuclear material, Tim Zimmerman & Alan Cooperman, The Russian Connection, *U.S. News and World Report,* 23 October 1995

advanced technologies. Traditional, terrorist and criminal organizations are structured in simple hierarchical designs, with a "great leader" or "Don" overseeing virtually all material decisions. The passing of information is performed in a managerial style that starts at the top and works its way down to the operators. As the information revolution continues to progress it appears to be lessening the need for middle management positions. Within a networked design, information can be instantaneously dispersed throughout the organization with the simple push of a computer key. The advantages of such a networked system were quickly realized and evidence has been collected that confirms its implementation.[32]

Criminal organizations have perhaps made the transition to new technologies even faster than terrorists. This may be due to the inherent business-like nature of criminal enterprise and the continued push for greater profits. These information systems have allowed for a more decentralized configuration consisting of numerous semi-autonomous cells that maintain a loose coupling to the command structure. This design allows for a percentage of the profits from every cell to reach the apex, while allowing increased autonomy, and thus criminal initiative, to thrive at the lower levels. A classic example of this structure is seen with the Chinese Triads. The loosely affiliated "gangs" are left virtually unsupervised to conduct business as they deem fit and are allowed to continue as long as homage is paid to the greater "Tong." Where at one time the operating pace of criminal organizations was constrained by a hierarchical structure that weighed the

[31] The organizational structure of terrorist groups and the trend toward a networked design is analyzed by John Arquilla, David Ronfeldt, and Michele Zanini, *Networks, Netwar, and Information-Age Terrorism,* (Santa Monica: RAND, 1999 forthcoming)

[32] Computers and advanced communications systems were observed in a camp run by Osama bin Laden, Hamas has set up Internet pages and uses e-mail and chat rooms to communicate and coordinate activities, and a raid in Italy discovered computer and communications equipment in a GIA (an Algerian terrorist

consequence of every decision, today's autonomous cells are free to determine their own restrictions. As greed and increased competition demand greater profits, these cells blatantly disregard local and federal law enforcement. The criminal organizations of the information age conduct any and all business in which they can make a profit, ignoring the self-imposed restriction of the hierarchy.

Similarly, terrorist organizations are converting to a network structure in an effort to enhance capabilities and expand areas of operations. Networked terrorist groups find themselves free from geographical constraints and the restrictive, time-consuming necessity to consult with leadership. While the network structure is being quickly embraced by professional groups, it has significantly advanced the trend toward amateurization, as discussed earlier. As the Internet allows groups to communicate freely around the globe, a call for violent action can quickly reach a receptive audience. This initial call may only present loose goals and guidelines and leave the more detailed decision making process, including target selection, to whoever wishes to take up the cause. This significantly decentralizes the organization, creating independent cells that no longer display loyalty to a leader but rather to a common goal. This design maintains anonymity through out the organization, making it extremely difficult for intelligence and law enforcement agencies to conduct counter operations. This structure is exemplified by the white supremacists in the US. The lack of centralized control produces a tendency toward engaging in a greater number and more destructive acts. This operational freedom is appealing to groups that view their actions as a form of war. For more specific goals, in which operations are conducted in accordance with an overall strategy, this networked

group) base. These are only a few of the examples which display terrorists willingness and capability to employ advanced information technologies, Arquilla, Ronfelt,& Zanini p. 26-27

structure is less appealing. Thus, terrorist organizations conducting actions on behalf of state sponsors are more likely to employ a hierarchical structure that can be more easily monitored and controlled.

Some of the older terrorist organizations, like the Abu Nidal Organization (ANO) and the Popular Front for the Liberation of Palestine (PFLP) have found it difficult to make this transition to a networked structure. This reluctance to shift designs may be due to the lack of familiarity with new information systems[33] and an aversion or fear of delegating authority to lower levels. The "younger" terrorist organizations like the Islamic Jihad and the al-Gama' at al-Islamiyya, tend to attract a younger generation that is inherently more comfortable and acquainted with information and communication technologies. While these younger organizations tend toward a networked structure, they are also seen to be more religiously motivated. Thus, it becomes difficult to determine whether the increased activity level is due to organizational structure or religious motivation. More likely than not, the result is a combination of the two.

Enhanced administrative capabilities and procedures have primarily propelled the shift to the networked organizations. The affordability of computers and the interconnectivity of the World Wide Web have made communications around the globe extremely easy, efficient and affordable. The advancement in encryption techniques has made it virtually impossible for intelligence agencies to intercept communications.[34] Even if governments were able to decrypt messages, their ability to act on them may be significantly hampered, if not prohibited by domestic and international law. The legal

[33] Arquilla, Rondfelt & Zanini p. 28

[34] There is a trend toward the employment of encryption by criminal organizations and the inability of the US government to keep up. An analysis of criminal use of encryption is provided by William Baugh and

right of any party, including extremist groups, to post home pages and conduct "chat rooms" greatly increases the capability to reach and influence thousands of individuals daily. The increased capabilities of faxes and cellular phones allow secure communications from virtually any location on earth. The incorporation of these information and communication-based assets has allowed terrorist and criminals to improve their efficiency by flattening their organizations and developing networked structures.

E. TACTICS

The operational tactics utilized by terrorists and criminals are representative of both their goals and capabilities. In the information age, these capabilities include the employment of conventional weapons, weapons of mass destruction and the relatively new netwar attacks. Actual use of these weapons is determined by the extent to which their employment will advance the organization's particular goals. For example, domestic terrorists, whose goal is to gain public support for internal change, would shy away from utilizing a WMD. The use of such a violent weapon would most likely isolate the group more than win support.

Traditional terrorist tactics have employed the gun and bomb as the staple of operations. A survey of terrorist incidents committed between 1968 and 1993 reveals that 46 percent of all attacks were bombing incidents, with another 22 percent being attacks

---

Dorothy Denning, "Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism," *Trends in Organized Crime,* Vol. 3, No. 1, 1997

on installations with conventional weapons.[35] These numbers reveal the probable terrorist intent to limit the number of casualties. In fact, less than a dozen attacks during this time period each claimed over 100 lives. Many experts believe that terrorists will maintain these tactics as their primary modus operandi.[36] This belief is largely based on the fact that these tactics have been and will continue to be effective. These weapons have proven sufficiently violent to provide the terrorists with the publicity they were seeking, yet tame enough to avoid alienating support. Thus, conventional weapons are seen to best fit the goals of the politically motivated terrorist.

While conventional weapons will continue to be employed by the professional terrorist, they also appeal to the amateur terrorist for numerous reasons. For starters, the skill level necessary to employ these weapons is normally quite low. Thus guns and bombs are suited to the amateur terrorist, whose skill level and ability to train effectively are also quite limited. With very little ability, the amateur terrorist is able to create "home made" explosives through directions provided over the Internet or in his hometown library. These weapons are also relatively inexpensive, which makes them attractive to the amateur terrorist who, for the most part, is self-financed.

When analyzing the prospects of a WMD attack, the terrorist's motives, skill level and financial resources must be considered. Many experts have written on this vital subject with the consensus being that employment for political motives is unlikely.[37] As

---

[35] These numbers were taken from Bruce Hoffman, "Responding to terrorism Across the Technological Spectrum," who summarized the data from The RAND Chronology of International Terrorism

[36] "[T]errorists will not engage in overkill if their traditional weapons – the submachine gun and the conventional bomb – are sufficient to continue the struggle and achieve their aims." Walter Laqueur, "Postmodern Terrorism," p. 31

[37] Jerrold Post, "Prospects for Nuclear Terrorism: Psychological Motivations and Constraints," *Preventing Nuclear Terrorism,* ed. Paul Leventhal & Yonah Alexander, (Lexington Books, 1987), pp. 91-103 & Joseph Pilat, "Prospects for NBC Terrorism after Tokyo," *Terrorism with Chemical and biological*

the motives of terrorists tend to transition away from politics and toward religion, the potential for a WMD attack increases significantly.[38] As mentioned previously, many religious-based terrorists regard their operations as an act of war that is blessed and justified by divine right. In execution of this "holy war," the use of any weapon, regardless of destructive capability, is viewed as appropriate.

While the religiously motivated terrorist may be more likely to carry out a WMD attack, WMD use by political actors can not be ruled out. Circumstances may arise in which these political terrorists find the employment of a WMD a completely rational and justified act. The ability to justify this action is largely determined by group psychology[39] and is impelled by the belief that the group's honor is at stake. This preserving or redeeming of "honor" may involve the desire to punish or seek revenge for believed misconduct.

While a terrorist group may utilize a WMD on its own behalf, an even greater fear is such use in the interest of a state actor. This scenario can be easily envisioned, for example, if Saddam Hussein were to feel that his fall from power was imminent. Another significant threat of a terrorist use of a WMD is its employment as a means of last resort. This is analyzed in a later chapter dealing with the danger of escalation. An additional threat that requires US attention is the potential use of a WMD for extortion purposes.

Weapons: Calibrating Risk and Response, ed. Brad Roberts, The Chemical and Biological Arms Control Institute, Alexandria VA

[38] "During the past decade, for example, religious terrorists or members of various religious "cults" have come closest to crossing the threshold of terrorist use of a *bona fide* weapons of mass destruction." Hoffman, "Responding to Terrorism Across the Technological Spectrum," p. 346

[39] Jerrold Post, "Prospects for Nuclear Terrorism" & Martha Crenshaw, "Decisions to Use Terrorism: Psychological Constraints on Instrumental Reasoning," *International Social Movement Research,* Vol. 4 1992, pp. 29-42

The ability to hold an entire city for ransom may be quite appealing to certain individuals or groups.[40]

Other factors, regardless of terrorist motivation, make concern about WMD attack necessary. The collapse of the Soviet Union and the subsequent degradation of security over its vast nuclear arsenal has virtually ensured the proliferation of nuclear material. Aside from nuclear material, the growing knowledge necessary to create chemical and biological weapons is in its own right an extremely disconcerting situation. In contrast to plutonium, that can only be used for nuclear needs, many of the chemicals used to create chemical weapons are also used in everyday materials like plastics. Thus, adequate control and tracing of these chemicals is simply impossible. While the creation of chemical or biological weapons by either professional or amateur terrorists is a significant concern, the large, state-run chemical weapons plants present an even greater threat. This threat increases drastically when states have already supported the conduct of terrorist activity, as is seen in the case of Libya. While the employment of such weapons is seen to be extremely difficult, as seen in the failed Tokyo subway attack, the knowledge gained from each failed attempt will improve the chances, ultimately, for a successful attack.

The advent of the information age, with its high-speed computer technology, has created an abundance of new opportunities for both terrorists and criminals. These non-state actors have quickly realized the advantages that these technologies are able to provide in the operational realm. Today's advanced computer systems provide the modern non-state actor with both targets as well as the weapons necessary to attack them.

[40] "In thinking about the possibilities of nuclear terrorism, it is important to distinguish between the actual detonation of a device and the use of a device for extortion and influence. The constraints against the latter

The advent of netwar in the repertoire of terrorists and criminals has significantly escalated their ability to threaten US national security. For this discussion, netwar will be used to apply to conducting disruptive, destructive or manipulative acts on information and communications systems. While all three actions (disruption, destruction and manipulation) are appealing to groups of all three of the motivations discussed at the beginning of the chapter, there is a natural pairing of the two.

Disruptive action in this context is defined as action which in itself does not cause physical damage or the loss of life. In this light, the disruptive technique of netwar is perhaps best suited to the needs of the political terrorist. Disruptive terrorist acts may include actions as simple as the spreading of a computer virus, or more significant acts like tampering with the control systems of commuter trains. Other disruptive acts could include: the implanting of an automatic link in the World Wide Web which visits the terrorist's home page and describes their plight and the injustices of the present government; the interception of satellite communications and the broadcast of propaganda over television and radios; or instilling uncertainty and fear in the world's financial markets by simply threatening or actually adjusting the prices of stocks and bonds. All these acts and many others would bring the terrorists, and thus their plight, worldwide attention while averting the need for any real physical damage. While these acts may have seemed farfetched a few years ago, they are legitimate threats today.[41]

Netwar allows these terrorist groups to regulate the magnitude, proportion, and range of their actions to best suit their needs. Thus, the conduct of disruptive netwar may

---

are significantly reduced..." Jerrold Post, "Prospects of Nuclear Terrorism," p. 102

[41] "A Nation at Risk, President's Commission on Critical Infrastructure Protection." Hearing before US Congress, Committee on the Judiciary Subcommitte on Technology, Terrorism, and Government Information, Nov 5, 1997.

initially save lives, since the terrorists have gained other ways of achieving desired attention. However, as the need for bigger and more spectacular acts becomes necessary, to grab media and public attention, more intense and alarming disruptive action may be performed. Inevitably, some of these politically motivated terrorists will feel compelled to resort to violent action. When this point comes, the conduct of netwar allows for an easy transition to destructive techniques.

The destructive technique of netwar is best suited to groups that desire to inflict casualties and physical damage without concern for their "image." As mentioned above, these are the groups that see their struggle as a form of warfare. Thus the religiously motivated terrorists are best suited, although by no means limited, to the use of the destructive capabilities of netwar. The destructive form of netwar utilizes the same basic principle as the disruptive technique but targets systems whose collapse or damage would create injury, structural ruin or death. Some potential destructive acts could include the intrusion into airfield computer systems in order to provide false landing information, or an assault on nuclear reactor control systems in the hopes of creating another Chernobyl. The terrorists would only have to cut off power to Chicago in the middle of winter to potentially inflict hundreds of deaths. Many additional and even more horrific examples can be provided. The list is virtually boundless.

Transnational criminal organizations are perhaps the biggest users of the manipulative capabilities of netwar. Manipulation, in this case, describes actions that are conducted for the benefit of the perpetrator without regard for their effect on outside parties. In other words, manipulative netwar, unlike the disruptive and destructive forms, is not necessarily performed to create an effect on a specific target.

The incredibly large daily volume of electronic data that is carried across information and communications systems has provided criminal enterprises two exceptional opportunities. Perhaps the more prevalent is the ability of criminal organizations to hide their illegal transactions among the huge flows of legitimate activity.[42] Transferring illegally obtained money was, at one point, a difficult process due to the sheer magnitude of money involved. Today, the same transactions can be completed many times over with the use of a computer. The ease with which criminal enterprises can launder money through use of advance computer systems is incredible. Money laundering today is estimated at $500 billion a year and is said to be the third largest business in the world.[43]

The second opportunity, presented by netwar manipulation, is the conduct of computer-based insurance schemes, fraud, and investment rackets. The U.S. Justice department estimates that computer based theft costs US businesses $10 million annually. Indeed, information technologies may be transforming the face of crime away from violent actions toward digital computer techniques.

As advanced technologies and expertise become increasingly available, both terrorists and criminals will rely more heavily upon the conduct of netwar. Until recently, the realm of cyberspace was relegated to the major business corporations that were able to afford the expensive hardware and train or hire personnel capable of using it. Today, the exponential rate at which the power of personal computers has risen while the cost of owning one has plummeted, allows virtually every individual the opportunity to enter into the information realm. While the threat from individual "hackers" performing

[42] The UNDCP estimates that $ 1 billion of illicit capital moves through the worlds financial systems on a daily basis, United Nations International Drug Control Program, Drugs and Development, No. 1, 1996

operations from their basement with a new Pentium II processor is a significant problem, the real threat to national security is felt from organizations that are able to purchase more powerful and capable information systems. As the tools to engage in netwar become increasingly available, the expertise needed to manipulate the systems continues to grow. These information and communications experts are being "homegrown" as well as being recruited from the best schools in the world. These non-state actors are willing to pay exceptional salaries to individuals possessing these skills and, once the job is accepted, the option to resign does not exist. In addition to computer experts, former intelligence professionals from organizations like the KGB have been employed to serve terrorist and criminal needs.

In addition to the increased offensive capabilities, netwar provides the non-state actor with numerous defensive benefits, including the decreased likelihood of apprehension. Perhaps the greatest defensive benefit to utilizing netwar is the lack of physical presence necessary to conduct the act. This distinct quality of cyberspace allows the terrorist or criminal to conduct operations in foreign countries around the world. As mentioned in a later chapter, these non-state actors take full advantage of the difficulties that face law enforcement in establishing jurisdiction. While these difficulties may be alleviated through administrative measures, the abilities of netwar render establishing a point of origin a tremendous problem in itself. As the information super-highway continues to expand, the ability to detect and trace the origins of any single transaction or process becomes extremely problematic, if not impossible.[44] This dilemma becomes increasingly more significant when the use of encryption is applied. While the US has

[43] Kerry, *The New War*, p.150

maintained the belief that powerful encryption should not be disseminated[45], the criminals and terrorists are already employing unbreakable encryption capabilities. Thus, while illegal organizations are able to safeguard their transactions, the legitimate businesses that are in danger from these groups are not allowed to do so.

F. CONCLUSION

Terrorism and crime are continuously evolving in an attempt to keep pace with societal changes and technological innovation. Terrorism, once thought to be solely political in nature, has found additional motivations, the greatest of which are religion and money. The expanded range of terrorist motivations and the increased cooperation between terrorist and criminal organizations has produced an exceptionally potent threat to US security. To add to the rising dilemma, these non-state actors have shown an attraction to and proficiency with advanced communications and intelligence systems. These technologies have precipitated the transformation seen in today's terrorist and criminal organizations. The rise of "amateur terrorists" from a trivial level to a serious concern can be substantially attributed to the ability of the Internet to put out "the word." The unprecedented ease of international travel and the security in long-distance communications have greatly facilitated the conduct of international terrorism and crime.

Perhaps the greatest employment of advanced intelligence systems has been in organizational restructuring. The trend toward networked designs has already displayed

---

[44] The effect that encryption has on law enforcement capabilities is discussed by Louise Shelley, "Crime and Corruption in the Digital Age," *Journal of International affairs,* Spring 1998

[45] A discussion on the dilemma the government faces on encryption issues is presented in Kerry, *The New War*, pp. 131-132

its ability to produce more efficient and effective terror and criminal organizations. In addition to the administrative characteristics, advanced technologies have provided these non-state actors with an extremely powerful weapon in the form of netwar, and an extremely target rich environment. Terrorists and criminals have adapted notably well to the information age, and in so doing pose a severe threat to American National Security. The US can no longer afford to regard these groups as a secondary threat which has traditionally taken a back seat to state actors. While in the past these threats may have been considered an inconvenience or a minor security concern, today they pose the most active and uncertain threat to the US and its interests.

III. CONTRASTING STRATEGIES

To confront the significant problems of terrorism and transnational crime, a wide range of tactics are available. While these tactics can be bundled together in a variety of ways to develop a wide range of overall strategies, they basically fall into two categories. These two distinct and fundamentally opposite categories are: reactive and proactive approaches to counter terrorism and crime. The reactive strategy is composed of four tactical groupings: prosecution, administrative measures, defensive measures and military action.[46] The proactive approach emphasizes the use of information operations in the conduct of disruptive and destructive acts.

Current US efforts to combat these growing security concerns are focused on reactive measures. The US policies of prosecution, no concessions, treaties, defensive posturing and sanctions are all tactics that allow the terrorist or criminal entity to retain the initiative. The objective of these tactics is to persuade, through indirect (and thus ineffective) pressure, the cessation of illicit activity. Even the seemingly aggressive use of military strikes, as was seen with the Tomahawk attack on the Bin Laden organization, in the manner currently employed, falls into the guidelines of a reactive strategy. Proof of the current US reactive strategy's ineffectiveness can be seen by the continued booming criminal industry and the recent domestic and overseas terrorist attacks.

---

[46] David Tucker in his article "Responding to Terrorism," *The Washington Quarterly,* Winter 1998, discusses 9 methods the US uses to respond to terrorism. This paper combines four of these methods: negotiating treaties and conventions, addressing terrorism causes, economic sanctions and policy of no concessions, into a single heading termed administrative measures. When addressing the two proactive measures of disruption and preemption, the US has, with limited exceptions, ignored their practice. The State Department's *Patterns of Global Terrorism,1997,* April 1998, only addresses three tactics; no concessions, prosecution and treaties, and conventions.

In order to combat and ultimately eliminate these groups as a significant threat, a more effective strategy is needed. A proactive approach with an emphasis on (IO) has the potential to provide this effectiveness. Through attacks, primarily non-lethal, at all levels of terrorist and criminal operations, the US can sufficiently deteriorate these groups' capabilities and reduce their appetite to continue operations. While the proactive approach provides a significantly more effective strategy for combating these threats, it also presents new and non-trivial costs. However, when analyzed against the costs of the current US reactive strategy, it is observed that these "new" costs are minimal and, over a short period of time, will present the US with significant "total" savings. A complete cost comparison analysis is conducted in the next chapter.

A. REACTIVE STRATEGY

The tactics employed by the current US reactive strategy are intended to influence the terrorists or criminals to cease operations, but do little to restrain terrorist and criminal options. Under these tactics, the terrorist/criminal is allowed the option to continue activity as normal, delay operations until pressure subsides, or, as the US hopes, terminate operations all together. The problem in this process is that it is the terrorist or criminal himself that currently gets to make this choice. This freedom to determine their own conduct cedes them the critical initiative and forces the US into a reactive posture.

The first component of current US efforts is the policy of prosecution. Prosecution, in this context, is the US government's effort to present the perpetrators of such action in front of judge and jury in the hopes of convicting and sentencing them.

Perhaps the most significant flaw in this tactic is that it is employed only after a terrorist act or criminal activity has been performed. Successful conduct of this tactic first requires knowledge of who performed the act, then to bring the individual or group into custody, then finally to convict them in a court of law. Not only does this tactic incur significant cost in both manpower and funding, it does nothing to prevent future action. Proponents of this policy argue that the example set by successfully convicting and subsequently incarcerating or even putting to death, these individuals will provide effective warning to future perpetrators. While this may be accurate in the case of the "wishy washy" terrorist, it has virtually no effect upon the religious zealot, the individual who sees himself as a martyr, nor the individual who believes he will not get caught. A terrorist who is willing to die in the conduct of his attack will not be swayed by the threat of a death penalty that will inevitably take years to carry out. When dealing with crime, the threat of incarceration seems minuscule as compared with the potentially huge payoff of successful operations.

Prosecution carries numerous additional difficulties to include extradition procedures and sovereignty law applicability. While attempts at resolving these difficulties are performed through administrative measures, as discussed below, terrorists and criminals are exploiting and hiding behind these problems to the fullest extent.

In addition to the difficulties of effecting such a tactic comes the potential that the perpetrators may be able, through skillful legal representation, to manipulate or abuse the US's legal system. The ramifications of such a scenario, in which an acquittal is delivered, would be devastating to future counter efforts and would significantly encourage rather than deter future action. The prospects for such a scenario are not too

remote when one realizes the monetary resources available to many of these organizations.

The US government currently relies heavily upon administrative measures to combat terrorism and crime. The primary administrative vehicles utilized by the US are international treaties, conventions and economic sanctions. While these tactics have their place within any complete strategy, they are rarely very effective as a method of directly combating terror and crime. These administrative measures may in fact facilitate the prosecution procedure. However that tactic, as discussed above has problems of its own.

While treaties, sanctions and international agreements played a significant role in curtailing terrorism in the 1970s and '80s, they have proven of limited value in the post cold war era.[47] Unlike the terrorist of the '80s, today's terrorist organizations are not as controlled or influenced by foreign state actors. While numerous rogue states still support terrorist organizations, some more covertly than others, they are either unconcerned with world opinion or are sufficiently economically and politically leveraged with other UN countries as to ensure their continued vitality.[48] When deniability or simple non-compliance with these treaties is in a state's best interests, economically or politically, it simply ignores them, as was seen in France in 1994.[49]

[47] "As has now been revealed in the wake of the collapse of the Soviet Communism in 1989, most of the international terror that plagued the world from the late 1960s through the mid-1980s was the product of an ad hoc alliance between the Soviet bloc and dictatorial Arab regimes." Netanyahu, *Fighting Terrorism*, p.53

[48] In 1996 French businesses disregarded US Congressional passed laws aimed at preventing foreign investment by threatening sanctions, by investing 2 billion in Iranian oil fields.

[49] In January 1994 the French Prime Minister released Iranian suspected terrorists wanted by Switzerland. Sharon Waxman, "France's Release of Iranians Triggers Swiss Complaint," *Washington Post*, January 1, 1994, p. A15

The reduced importance of administrative tactics can also be explained by the significant shift seen in terrorist motives.[50] This shift is away from the earlier period of politically-based terror and toward religious and economic terror. The goals of the political terrorist required that they take into consideration the effect their actions would have on external opinion. In fact, many of their acts were conducted for the very purpose of affecting foreign opinion. On the other hand, economically motivated terrorists escalate their tactics as necessary to ensure their monetary prosperity. The religious terrorist sees himself as fighting a holy war in which the external influences themselves are often what they are fighting. This religious motive demands additional scrutiny and concern, since their goal may very well have limitless destructive intentions.

The introduction of cyberterror and crime plays havoc with and virtually renders impotent a number of current US reactive tactics.[51] The nature of cyberspace, which is borderless, or conceptually non-existent in the geographic sense, virtually eliminates or at a minimum significantly confuses the effectiveness of international treaties. While the laws within the US are having a difficult time getting a handle on this "new" instrument of terror and crime, the majority of other countries haven't even addressed this problem.[52] Thus the difficulties in determining jurisdiction and which nation's law to apply, if indeed they have laws of this nature, are immense.

---

[50] Medd, & Goldstein, "International Terrorism on the Eve of a New Millennium"

[51] While the definition of terrorism is itself a difficult matter, cyberterror or information terrorism is even more so. Martin C. Libicki in his essay, *What is Information Warfare?,* (The Center for Advanced Concepts and Technology, 1995), pp. 75-77, defines it in very narrow terms as a subset of computer hacking. Cyberterror, viewed in a much broader form and possessing significantly greater consequences, is presented in a short story by John Arquilla in *Wired* magazine, Feb 1998.

[52] A discussion on the legal aspects of Information Warfare is provided in Richard Aldrich, *The International Legal Implications of Information Warfare,* (Colorado Springs: Institute for National Security Studies, 1996)

The US use of administrative measures to fight international terrorism has many shortfalls. However, when dealing with domestic terrorism, the US wisely structured its laws and law enforcement offices to avoid many of these same problems. Designating terrorism as a federal offense, vise a local or state offense, solved both jurisdiction and law applicability issues. The Federal Bureau of Investigation, by federal law, possesses jurisdiction over all domestic terrorist acts.[53] Thus, unlike in the international realm, administrative turf battles are a much less powerful factor in domestic affairs.

While the use of administrative measures is seen to have a limited effect upon international terror, it bestows even less upon the transnational criminals. A primary reason for this ineffectiveness is the inability of many foreign governments to exert any measure of control or significantly combat these organizations within their own territory. Relatively few foreign countries, from which these criminal organizations originate, possess a proficient police force capable of performing sufficient law enforcement. This is most drastically seen in Colombia, and more recently in Russia. Thus, while states themselves may be more than willing to cooperate with international agreements, they are unfortunately often incapable of doing so.

At the other extreme of criminal-state relationships, are countries that benefit from criminal activity. These are the countries that provide secure banking facilities for criminal organizations to launder their money. In many of these countries, official secrecy of offshore financial centers is written into law[54]thus preventing cooperation in

[53] GAO report, "Combating Terrorism," Sep 97, Federal agencies efforts to implement national policy and strategy

[54] Kerry, *The New War*, p. 155

international agreements. Perhaps the most notable case of this government/criminal cooperation was seen in Panama under Manuel Noriega.[55]

While the ability of some foreign governments to prevent criminal action may be severally limited, cooperation treaties have shown the potential to improve world law enforcement efforts. The agreements to allow FBI agents in foreign countries to advice and work in cooperation with foreign government police forces is a step in the right direction.[56] While this cooperation has produced some successes, the decline in total criminal activity produced from these successes is literally non-existent. The reason for this poor result is the inability of even combined efforts to significantly penetrate the numerous criminal organizations.

The third tactic within the current US reactive strategy is reducing vulnerabilities through increased defensive measures, awareness and training. Perhaps the most visible effect of this reactive strategy, and a fairly symbolic one, is the ever increasing emphasis on hardening overseas facilities.[57] Through the implementation of crash walls, multi-tiered wiring, security gates and numerous and varied sensors and detectors, the US has attempted to insulate itself from terrorist attack. This tactic fails in two respects: one, it doesn't work; and two, it imprisons the wrong people. Regardless of the amount of

---

[55] "Using the Panamanian banks, dictator Manuel Noriega created a civil regime indistinguishable from a global criminal gang, where the state and its bankers sponsored drug and arms trafficking and prostitution, as well as engaging in money laundering and tax evasion," Kerry, p. 157

[56] FBI director Louis J. Freeh, discusses the successes of current and planned cooperation agreements between his agency and numerous foreign police forces in front of the committee on International Relations of the House of Representatives Oct. 1, 1997

[57] It is difficult to determine the exact spending levels of government agencies on anti-terrorist activity. This is true due to the definitional problems, agencies tend to include anti-terror expenses into larger categories, and agencies are not required to account separately for their terrorist related programs and activities. However, as described in the GAO report GAO/NSIAD-97-207, "Combating Terrorism, DOD efforts to protect its forces overseas," Jul 97, the DOD estimates that it spends over 4 billion dollars

defensive structuring, terrorists have always been able either to find the weak point, or simply to find a more vulnerable target. As the US enhances defenses around military bases and embassies, terrorists have shown a trend to target US business personnel, individuals on vacation or private businesses that are associated with the US or the American way of life.[58] Perhaps an even more alarming prospectus is that the implementation of these point defenses may drive terrorists to stand-off weaponry and increasingly more powerful explosives. This weaponry may include the use of biological and chemical agents as well as nuclear devices. In addition to the inherent ineffectiveness of defensive measures, the heavier security procedures significantly hamper and inconvenience the personnel they are intended to protect.

The second component to this tactic consists of educating high-risk personnel as to the level and type of threat, and subsequently training them how to avoid being a target.[59] The US has spent significant effort and money to better inform and train its overseas personnel in hopes of minimizing vulnerabilities to terrorist attacks. Regardless of the extent and efficiency of this training, terrorist acts will continue to occur. Terrorists committed to carrying out their attacks will inevitably find a fatal flaw.[60] Terrorists have the luxury of being patient and waiting for their targets to make a slip. In addition, terrorists are generally afforded the time to reconnoiter numerous potential

---

combating terrorism. The same report states that while security improvements have been made, significant vulnerabilities still remain.

[58] 104 out of 126 terrorist attacks in 1996 targeted business personnel, "Patterns of Global Terrorism, 1997", United States Department of State, April 1998

[59] As stated in GAO/NSIAD-97-207, DOD's antiterrorism Program , "DOD has mandated more robust antiterrorism training for personnel deploying to medium to high threat countries. The training is intended to increase awareness of the threat and provide information on individual protection measures."

targets and simply pick and choose who and when. While training and education may cause the terrorist to extend considerably more effort than would have otherwise been needed, it does not inhibit performance.

In the criminal arena, government programs to educate the American populace on the detrimental effects of crime have done little in the way of curtailing activity or limiting victims. The government's largest effort in this area has dealt with the use and distribution of illegal drugs.[61] While this is a noble endeavor it has proven to have a limited effectiveness. Criminal organizations have developed new marketing schemes, including introduction of drugs to very young children, and the introduction of highly addictive drugs.[62] These criminal efforts have outpaced the government's education and prevention efforts.

While the drug trade is one of the more prevalent criminal enterprises, it is definitely not the only one. In the areas of smuggling, racketeering, prostitution, fraud, etc., efforts in education and awareness are minimal, and are seen to provide extremely limited defense. Many times, the only education provided to the American people is on popular news shows like *Dateline* or *20/20*. The primary reason for this lack of government concern is that crimes like mail fraud and insurance scams are not seen as a serious threat.

---

[60] An excellent example is Col. James Rowe, who, as an Army Special Forces Officer, had received some of the best training in this area, yet on April 21, 1989, he was ambushed and killed by the Philippine "New Peoples Army" while traveling to work outside Manila.

[61] The President requested 1,916.5 billion dollars in fy98 for drug prevention efforts, and 3.003 billion for treatment, "The National Drug Control Strategy, 1997: Budget summary", The White House, Feb 97

[62] Use of illicit drugs among 8th graders is up more than 150% over the past 5 years. "The National Drug Control Strategy"

The final reactive tactic utilized by the US is the performance of limited military strikes against suspected terrorist camps and facilities. While this tactic may initially look like a very aggressive proactive measure, deeper analysis reveals its true reactive nature. The primary goal of these operations is to persuade terrorists and state sponsors to cease further operations. As stated previously, this is a reactive goal that leaves the option, and thus the initiative, in the hands of the terrorists. As discussed further below, the US has only used this tactic to punish terrorist organizations for actions that have already been committed and lives already lost. It seems that the current US position adopts this reactive stance in the hope that the eventual counter attack will seem more justified.

While these military strikes grab headlines, the actual benefit of such action is arguable. Successful strikes have the potential to completely destroy and incapacitate terrorist training camps and facilities, but the damage incurred is primarily structural and quite easily replaced. Additionally, if the strike does not completely destroy the terrorist's capability and the will to perform further operations, the desire for retribution will be enormous. With the trend toward more powerful weaponry, including WMDs, retribution for such an attack may be excessive. The US government may also incur enormous costs in world opinion. While the domestic constituency will normally see this action as appropriate and justified,[63] the world opinion may not be so friendly and potentially may be less willing to cooperate with the US on future matters.[64]

[63] The strikes on the Bin Laden terrorist facilities had the support of 3 out of 4 Americans. "The military strikes have boosted Clinton's political standing and public confidence in his ability to function as President", *LA Times* Aug 23 1998.

[64] For example, the strikes on Bin Laden's facilities were condemned by most Arab countries and by Russian Pressident Boris Yeltsin.

While the use of military strikes has historically been quite limited, two attacks have occurred in response to terrorist action. These cases are the air raid on Libya in 1986 and the 1998 Tomahawk strikes on the Bin Laden terrorist facilities. Both strikes were retaliatory in nature, performed in response to successful terrorist attacks. While the long-term results of this most recent strike are still to be determined, the Libyan results can now be sufficiently analyzed.

While the two strikes seem to be similar in nature there are two distinct differences that need to be addressed. In 1986 the US attacked facilities that were owned and operated by the state of Libya itself. In 1998 the strikes targeted facilities that were run by a non-state organization within the territorial boundaries of two countries. Striking a state itself is significantly less complicated than attacking an organization within a state. When striking a state entity, violation of sovereignty is not an issue, because it is the state itself that is the target. When striking a non-state player within the territory of other states, the violation of sovereignty becomes a very significant issue.

The second significant difference between the 1986 and 1998 strikes, is the accuracy of weapons used by the US. In 1986, the delivery methods and weapons accuracy virtually insured that damage would be inflicted upon unplanned targets. However, as mentioned above, since the target was the state itself, this collateral damage was much more palatable. In 1998, the pinpoint accuracy of the weaponry was critical, especially within the urban area of Khartoun, in Sudan. Any level of collateral damage during this strike would have brought significantly more pressure and admonition from world opinion.

The conduct of military strikes, and thus the threat of future strikes, is more effective as an instrument of deterrence when dealing with state actors such as Libya. This is true because Libya, as a country, can not pick up and move underground. It is always exposed to attack. Non-state actors such as Bin Laden have the luxury of mobility and elusiveness. Because of these factors, non-state actors are significantly harder to deter with conventional military strikes. Even in the case of Libya the success at deterrence is arguable, with terrorism having eventually returned to normal in the aftermath of Pan Am flight 103.[65]

Analyzing the use of lethal force against criminal organizations requires drawing a distinction between domestically-located and foreign-based strikes. On the domestic side, law enforcement is severely constrained by US law and a reluctance to use force due to social disapproval in this country. In addition, striking at the domestic aspect of international crime is similar to cutting off the tail of a skink, in which the lost appendage only grows back stronger. Combating crime overseas requires cooperation with the host nation, and very rarely involves actual force by US entities.

The US reactive strategy to terrorism and crime is clearly inappropriate in today's high risk, technologically advanced environment. Incorporating this reactive strategy allows the terrorist or criminal to retain the initiative. With this initiative, they are able to innovate around current US efforts aimed at stopping them, and are allowed great freedom of maneuver. Terrorists are able to plan, recruit, and solicit support with virtually no fear of reprisal or intervention until after lives are lost. Criminal organizations are laughing all the way to the bank while undermining American society.

[65] Tucker, "Responding to Terrorism," p.111

Thus, a significantly more aggressive and effective method is required. The advent of information operations has presented the US with the weapon it so vitally needs, not only to combat but to win the war against both terrorism and crime. IO, utilized within a proactive strategy has the capability to confront and attack these groups at their most vulnerable points. This proactive strategy will keep the terrorists and criminals on the defensive, forcing them to fear for their very existence and take away their ability to plan, and perform operations. While the proactive strategy takes a more aggressive approach, it does not abandon the tactics employed in the reactive strategy. The proactive strategy takes full advantage and utilizes all tactics available including the more administrative and reactive ones described above.

B. PROACTIVE STRATEGY

Although the proactive strategy retains many reactive tactics, it relies more heavily upon the two tactics of preemption, and disruption. Both are critically reliant upon accurate, precise and timely information. IO is thus a two-pronged instrument. The first prong provides one of the more important weapons in the actual conduct of operations. The second provides the tools necessary to gain the information that is required to properly utilize these weapons.

Preemption is the conduct of direct offensive action utilized to disable a terrorist or criminal organization's ability to perform a specific act or operation. The preemptive tactic can be equally effective against terrorists and criminals. However it is within the terrorist realm that the greater benefits are possible. This is true due to the potential

impact of a successful operation from a terrorist attack, versus the completion of a criminal operation. This point becomes abundantly clear when the concept of a terrorist's use of a WMD is considered.

Unlike the responsive military strike, the preemptive tactic is performed in expectation of a terrorist act. Thus, the US heads off the attacker, beating him to the punch, and subsequently averts the loss of innocent life. The use of preemptive measures eliminates the controversy behind responsive proportionality by creating conditions that force the abandonment of terrorist operations. In addition, the preemptive tactic utilizing IO, is much better suited to combat cyberterror, allowing the US to confront the terrorist at the same level, with the same and even better weapons.

In the context of terrorist activity, the preemptive tactic has many applications, all of which rely upon the knowledge of highly specific details. The creation of this condition can be accomplished in numerous ways, the specifics of which are explained in chapter 5, and only lightly touched upon here to help delineate the proactive strategy. It is important to note that many of these actions can be very effective without their employment being broadcast, or the loss of life being necessary on either side. Performing these operations clandestinely, and performing them in such a way that the terrorists do not even realize that they are being targeted, diminishes the threat of retributive attacks that are so prevalent with traditional military strikes.

Terrorist activity is inherently time sensitive. Any delay in any phase of the operation can throw off the timing so that the entire plan must be abandoned. The use of IO can create such delays in numerous ways. Knowing terrorists' intended travel and movement plans will allow the ability to prevent or delay such movement. The

cancellation of airline tickets or the flagging of passports can prevent travel or entry into or out of a country. Detaining or arresting personnel for necessary time periods, for virtually any reason to include loitering, can force them to miss their window of opportunity. A tactic as simple as informing the terrorists that we know of their plans, down to critical details would have a sufficient effect to warrant their cancellation. More active measures such as jamming communications, or entering into their intelligence network, can provide enormous opportunities. The impersonation of terrorist leadership that gives conflicting orders, or simply calls off the operation, can avert disaster. Tampering with equipment, including the weapons themselves as well as communications, vehicles, and money supply can all disrupt terror. Overt police presence, which virtually shadows the potential perpetrators, may make them realize the futility of their plans. These techniques, along with numerous other psychological operations, and even the occasional use of limited force, may both convince and prevent the terrorist from acting.

The tactic of disruption attacks terrorists and criminals at their origin, affecting their ability to plan coordinate and carry out future operations. This tactic is truly the core of the proactive strategy, taking the fight to the terrorists and criminals, placing them on the defensive. These disruptive measures, which focus on IO, have the ability to affect the terrorist or criminal organization at three levels: the international/state level, the organizational level and the individual level.

At the international level, the emphasis is upon disrupting sponsor and cooperative relationships in an effort to isolate and or alienate the terrorist or criminal organization. Many terrorist organizations rely, in some degree, upon the support or at a

minimum, the indifference of a state entity. This support allows the terrorists to organize and train behind the relative safety of state protection. In return, these organizations provide the state with a potential tool for clandestinely carrying out desired goals. While occasional exceptions have occurred, like the recent Sudan and Afghanistan strikes, US resolve to reach out and strike these targets in foreign territory is very limited. As mentioned above, the actual lasting benefit from these types of overt attacks is highly arguable. In addition, the potential lack of support from Congress is always a concern, and has the potential to cause political turmoil. Knowing these drawbacks, terrorists groups continue to rely heavily upon these support relationships. The use of disruptive IO techniques to erode this relationship, and subsequently to force these organizations to seek new "homes" avoids these problems and can significantly enhance counter terrorist efforts.

With respect to international crime, the criminal organizations do not seek this same type of relationship with state sponsors. Instead, criminal organizations take advantage of a weak state's inability to prevent their continued operations. While these foreign states may prefer to expel these groups, they are often incapable of doing so. Because these states are sovereign entities and possess national pride and political ideals, they will not allow unilateral US operations within their country. Thus, criminal organizations benefit from the same "safe haven" concept as the terrorist organizations. While progress has been made in the area of cooperative police activity, it is still significantly hampered by cultural and capability variations between the US and others. In addition, some state's offices and officials, as exemplified by Colombia and Russia, have become sufficiently corrupted and controlled by these criminal groups that

cooperation with US is severely hampered. Because of this relationship in which the criminal organization virtually forces its will upon the state, disruptive IO techniques are limited, but by no means useless.

While cooperation between states and criminal organizations may be actually weakening in some cases, the cooperation between criminal organizations themselves is growing stronger.[66] This inter-organizational cooperation, while posing a potent threat to the US, also opens up new vulnerabilities. A full discussion describing the capabilities of disruptive techniques is provided in a later chapter and only briefly mentioned here.

The goal of disruptive IO methods is to erode this support and cooperation. This can be performed in myriad of ways, limited only by one's imagination. One disruptive technique at this level could be the interception of monetary support or equipment transactions through computer systems. Providing the terrorist group with significantly less money, or no money at all, can quickly cause dissension. The planting of information which would indicate betrayal by the government, or the reverse, in which the terrorist organization that would conduct operations against its supporters can drive a wedge between entities. In the case of Arab-based terrorism, the false dissemination of information, or even doctored video depicting the group conducting acts that go against their religion, can quickly cost the group constituency support. Between criminal organizations, simply the belief that one organization has cheated the other will quickly cause a break in cooperation if not a "war." These and many other concepts are discussed in greater detail later.

The next level of disruptive operations is organizational. Both terrorist and criminal organizations are greatly affected by and reliant upon group dynamics. These group dynamics are centered on interpersonal relationships,[67] reputations, power, and ego. Due to the nature of both terrorism and crime, loyalty and trust are critical aspects of maintaining group cohesion.

The objective of disruptive IO would be to chip away at these areas with the effect of critically damaging these bonds. Artificially instilling paranoia into leadership levels can achieve this erosion, calling into question the loyalty and trust of group members. Inserting misinformation that would create an internal belief in a challenge for leadership can quickly cause dissension, factionalism, or even a "civil war." The leaking of information, although potentially false, that would seriously bring into question leadership ability or authentication of objectives, could reduce loyalties, support and future recruitment.[68] Perhaps an even greater effect on recruitment and retention can be accomplished through embarrassing the organization in the eyes of its constituency.[69] Once again fostering the belief of embezzlement or theft from one another has the potential to cause huge internal conflicts. Numerous other techniques are discussed later, but the key to all methods is to keep these organizations sufficiently busy with internal turmoil so that their operations become inefficient, and potentially cease altogether.

---

[66] "Not only have the Chinese become the world leaders in trafficking in heroin and fake credit cards, they have also sealed alliances with the Japanese Yakuza, the Russian Mafia, and the Colombian cartels through their expatriate network." Kerry, *The New War,* p. 64

[67] Martha Crenshaw, "An Organizational Approach to the Analysis of Political Terrorism," *Orbis* Volume 29, number 3, Fall 1985, p.474

[68] Jerrold M Post, "Narcissism and the Charismatic leader-follower Relationship," *Political Psychology*, Vol 7, No 4, 1986 p.676

[69] Directly effects the incentive of Social Status as described by Crenshaw, "An Organizational Approach to the Analysis of Political Terrorism," *Orbis* p. 478

The remaining level of disruption is at the individual level. This approach plays significantly on psychological operations, and can be broken into two general categories. The first targets a specific individual and is aimed at directly influencing his/her actions. The second utilizes and manipulates one individual to influence the actions of others.

Targeting an individual is intended to change his actions, beliefs, and desires. This includes the potential use of subliminal messages, in which the individual is continuously bombarded with subconscious images favorable to US desires. While the use of bribes, blackmail, and threats may also influence the individual into "seeing things our way," they probably have limited effectiveness with terrorists and criminals and have a high probability of backfiring.

The second category provides a dual benefit. First it takes the specific individual out of the picture, but more importantly it influences other individuals, the existence of which may not even be known. The two primary operations within this category are "snatches" (also known as arrests) and "extermination." While a trend toward networking has become evident (see chapter 4), some terrorist and criminal organizations are still centered around a few key individuals. In some cases it is the individual himself that keeps the organization alive by providing both the practical functioning structure as well as a spiritual idealistic leadership. Once an individual of this nature is abducted, significant image manipulation can be performed so as to alienate his constituency. This was seen to be the case with the Shining Path in Peru, in which the organization for all intents and purposes deteriorated after Guzman was captured and imprisoned. The Peruvian government, under President Fujimoros direction, enhanced this success by disseminating images and messages of an imprisoned and spiritually beaten Somosa . The

same principle can be seen in the case of criminal activity with the killing of Pablo Escobar, after which the Medellin cartel lost its prominent position to the more refined Cali cartel.

C. CONCLUSION

In 1997, there were 123 anti-US terrorist incidents.[70] The drug trade alone has accounted for over 16,000 American lives and cost taxpayers over 17 billion annually[71]. Clearly, US efforts to combat these serious security threats have been inadequate. A strategy in which America dictates the moves and attacks at the core of these phenomena is now within our capabilities. This proactive strategy focuses on the use of IO and strikes these groups at the three levels where they are most vulnerable. By adopting this unconventional approach to terrorism and crime, we could erode the "comfort zone" that terrorists and criminals now enjoy. Terrorism and crime are becoming an ever-increasing security issue. The US must implement this strategy and effectively reduce or eliminate these phenomena.

[70] "Patterns of Global Terrorism"
[71] National Drug Control Strategy

IV. COST OF DOING BUSINESS

With any proposed strategy, there are two key factors that inevitably determine its acceptance or rejection. These factors are effectiveness and cost. The first factor was the topic of chapter three; the second is dealt with herein.

Implementation of any strategy, regardless of its goal, will inevitably generate an inherent cost through the expenditure of some asset. This expense or cost can take myriad forms. Perhaps the most common expense is monetary or economic. This concept of cost applies whether one is buying a pair of shoes or fighting a war. In either case, the expenditure of resources is required. The resource that is consumed does not have to be monetary or even a tangible asset.

When dealing with counter terrorism and counter crime, the potential cost involved in any strategy is a critical factor in determining whether to implement it. If it were not, the US could simply conduct a nuclear strike into the heart of the Colombian drug cartel's cocaine production and eliminate it as a security concern. When sufficiently analyzed, the costs associated with carrying out such an action, (particularly the political costs) would undoubtedly outweigh the benefits. Thus, it is insufficient to focus solely on potential benefits of a given strategy. A proper analysis of the counter terror and crime strategies must heavily weigh the costs involved within each.

Analyzing the costs associated with terrorism and transnational crime reveals seven major cost factors. These factors are discussed in detail below in order to provide a greater understanding of their individual effects upon the likelihood of strategy acceptance. This cost analysis will provide a general and plausible outline that can then

be tailored to any situation. The significance of any cost is a relative concept determined by the judgment of whoever conducts the analysis. In other words, the loss of a $100,000 shipment of drugs may seem like a tremendous loss to the neighborhood drug dealer but is seen as inconsequential to the drug cartels.[72] In addition, the risks posed by engaging a particular strategy are included in the individual cost factors.

Each of the seven cost factors below is analyzed with respect to current US reactive strategy and the proposed IO-based proactive strategy. In order to perform this analysis properly, the costs must be observed not at a specific time and point, but over a more extended time period. The reason for this requirement will become abundantly clear as the analysis is conducted.

After each of the cost factors is individually analyzed, a cost diagram depicting the aggregate cost of all seven factors will be constructed for both terrorism and crime. The total cost difference between the reactive and proactive strategies can then best be observed. While there may inevitably be some bias as to the degree of significance of each cost factor, the principles and ideas that these costs are based upon remain relevant. In addition, the degree to which each of the strategies is implemented will affect each cost factor. In other words, the cost associated with any tactic will be in direct relationship to how aggressively that tactic is used.

[72] Annual turnover is estimated at $ 5oo billion by the United Nations Drug Control Program (UNDCP), United Nations International Drug Control program, *Drugs and Development*, no. 1 (1996) p.1

A. HUMAN LIFE

The value of a single human life is a concept that will most likely never be agreed upon.[73] Religious institutions like the Catholic Church will argue that human life is more important than any other issue- in essence, priceless. Governments, on the other hand, do not seem to value human life to the same degree. Even in democratic countries like the United States where human rights issues draw a large constituency, the value of life is, in practice, negotiable and varied. As proof of this belief, one need only look at the number of lives that have been lost in America's numerous wars and its embarrassing history of slavery. While governments tend to price life as less than of paramount importance, they are by no means the lowest bidders. The violence observed in inner city gang neighborhoods has shown virtually a complete disregard for human life. Gang initiations have included the blatant and random killing of innocent individuals whose only crime was being in the wrong place at the wrong time.[74] This disdain for human life is not relegated to the US alone, and numerous atrocities have and will continue to occur around the world. Perhaps the most horrific was the Jewish holocaust during World War Two. While the value of life is hard to quantify, some criminal groups do attempt to place a monetary value on life as seen in the cases of indentured servants and kidnappings.

---

[73] In Pope John Paul II's 11th encyclical, *Evangelium Vitae*, titled "The Gospel of Life" March 25 1995, he calls the value of human life "inestimable." On the other hand, an OMB report drafted in the 1980s by accountant John Morrall calculated the cost per life saved for various federal regulations. In essence placing a value upon human life. His estimates ranged from $100,000 to $72 billion.

[74] As an example of the sheer number of atrocities associated with gang initiations, the Lexus/Nexus research data base's search engine was overloaded by the number of newspaper reports on gang initiation violence even when limited to the past 90 days. In addition *The Journal of American Medical Association*, released a study in 1995 that charted an astonishing overall rise in gang murder, These murders accounted for 43% of all homicides within the Los Angeles area. 1/3 of these deaths involved individuals not associated with gang activity.

When attempting to justify US policy, the value of human life must be observed not at the individual level but at the state level. Thus while the loss of a loved one may be devastating on the personal level, it can be less consequential at the level of the state. The cost of human life at this level of analysis is affected by several factors, the greatest of which is the role of the media and the public opinion that it influences.[75] While media influence is closely related to the costs of reputation, as described below, it is important to expand on the concept of human life here, in order to understand its significance fully.

The value that the US government as an entity of itself places on human life varies significantly according to the context surrounding the loss of that life. When associated with terrorism, the value of human life tends to increase drastically. While the loss of a life in an overseas murder hardly raises an eyebrow, if the murder was somehow connected with terrorism it would inevitably create significant attention. The media plays a large role in this process. Murders, it is sad to say, happen hundreds of times a day and are deemed virtually unworthy of media attention. Terrorism, on the other hand, is deemed an extremely newsworthy event and will most likely be reported by the media to the fullest extent possible. This includes interviews with the victim's family and friends. This type of media attention creates enormous public outcry and consequently impels politicians to address the issue.

When associated with criminal activity the value of a single human life, at the level of the state, is seen to decrease drastically. In part, this devaluation is due to the routine occurrence of crime-related deaths. In the United States, a person is killed every

[75] The role that the media plays is discussed in depth by Bridgitte Nacos, *Terrorism & The Media*, (Columbia: 1994), especially ch. 2.

27 minutes from crime-related activity.[76] The American public has become numb to the tragedy of such incidents, and this numbness is transferred into the attitude of the federal government. Except for a few high profile cases, these deaths are considered routine, and thus accepted.

While the government may deem the individual life of a crime victim as of minimum value, the sheer number of deaths due to crime creates a cumulative effect, and has created concern and attention at the federal level. This concern is seen in the increased number of gun control initiatives and attempts at instituting stiffer punishment for gun related crime. Thus the cumulative value of life *is* significant and warrants governmental concern and action.

This discussion of the value of life has thus far only taken into consideration the actual loss of life. In order to fully grasp the cost of individual lives, we must also include the significant cost associated with injuries. In some respects, the wounded actually present a more significant cost than those that are killed. These costs involve hospital care, increased publicity, physical rehabilitation, government entitlements, and mental anguish. An example of this cost is seen in the injured William Brady, who has championed gun control measures since his shooting in 1981. This discussion is not intended to argue the merits or faults in gun control, but only to indicate that a cost in resources, time and money was, and continues to accrue, due to an issue that can be significantly attributed to the efforts and publicity of an injured individual.

In comparing the current US strategy with the proposed proactive strategy, we see that the potential savings in lives and injuries under the proactive strategy can be

[76] U.S. Department of Justice, Federal Bureau of Investigation, "Crime in the United States, 1996," *Uniform Crime Report,* dated 28 Sep 97

significant. As mentioned in the previous chapter, the proactive strategy incorporates the tactics of the reactive strategy and then adds more effective tactics that would foster a reduction of human costs. While the individual value of a life will remain the same under either strategy, the cumulative total will decrease in proportion to the number of lives saved. When the concept of a WMD terrorist attack is considered, these savings would be exceptional and by itself warrants incorporation of the proactive strategy.

B. MATERIAL DAMAGES

The discussion of material damages is broken up into two categories. The first is the cost to actual structures, and is thus the more tangible. The second is categorized as the cost of operations, and includes such factors as loss of business, knowledge and investment.

The damage inflicted upon physical structures can be visualized, and photographed. The cost can normally be measured monetarily and, in most cases, the structure can be rebuilt. This cost is primarily associated with terrorist bombings. In some cases, the cost is relatively small, as would be the case with a small car bomb intended to kill the occupant. More significant structural cost, however, was seen in both the Oklahoma Federal Building and the New York World Trade Center bombings. With the trend toward more destructive explosives, which could potentially include a small nuclear device, the potential cost of structural damage could easily skyrocket.

Perhaps even greater than the cost of structural damage is the cost of operations. This cost applies equally to terrorist and criminal activity. A terrorist bombing attack will

inevitably affect the ability of some legitimate organization to function as normal. Even if the attack were carried out at a personal residence, numerous resources will be diverted from their intended purpose. This cost may include the elimination or detention of an individual who would otherwise be productive. While the actual terrorist destruction of business operating spaces or the diversion of assets is a significant cost, it is by no means the only one. The loss of operating ability due to terrorist activity can be seen in numerous other ways.

The threat of a terrorist attack is in itself a detriment to business. As was seen recently in South Africa, the bombing of businesses that are even remotely associated with the US will have a deterrent effect to overseas investment. Another cost that is associated with either the destruction of business spaces or the killing of an individual is the loss in knowledge and experience. The destruction of business spaces may also include the loss of important documentation, computer files and business transactions, and is a cost that, in some cases may never be recovered.

On the criminal side, the cost of operations is a little more indirect yet potentially more significant. Criminal organizations impinge on legitimate businesses in several ways. The most obvious are extortion and theft through both traditional and more innovative methods (as described in chapter 3). Crime organizations also impede the success of legitimate businesses through the operation of their own cover or front operations. These criminal fronts often conduct legitimate business through illegitimate means. These operations are not intended to make a profit, but rather to hide illegal money. This disregard for profit places legitimate businesses at a disadvantage since they must make a profit or risk going out of business.

By preventing a significant number of terrorist attacks through preemption or disruption, the costs of material damages might drop significantly. By attacking the criminal organization through IO techniques, their ability to maintain cover operations and conduct business as normal would deteriorate, thus allowing legitimate businesses the opportunity to succeed. With respect to this cost factor, it is a simple equation of less terror plus less crime equals less cost.

C. REPUTATION

The first two cost factors, human life and material damage, are relatively tangible concepts in which the damage attributed to these factors can be observed or calculated. The remaining cost factors are less tangible. While a dead body is difficult to ignore and is relatively indisputable, the damage done to one's reputation is highly arguable. In an attempt to analyze the cost of reputation, a division between domestic and foreign reputation is conducted. For this discussion, reputation, both foreign and domestic, is associated with the government's ability to effectively counter-terrorism and crime as well as the perception of performing these tasks in a "just" manner. This "just war" concept goes directly to the issue of ethics.[77]

In the domestic realm, perhaps the most important issue that forms the government's reputation is specifically how well it can protect its citizens and their interests. America has long thought of itself as isolated from foreign aggression. With extremely limited and insignificant exception, the US has not faced a significant attack

[77] This is discussed in John Arquilla's "Ethics and Information Warfare," National Defense Research Institute, (forthcoming 1999)

from foreign forces since the War of 1812.[78] Americans have become accustomed to this perceived safety, and an enormous outcry and call for action arise whenever this security is breached. This is true whether the attack is carried out by domestic sources, as with the Oklahoma bombing, or from foreign influences as with the Trade Center bombing. The American public believes strongly that the US is without question the preeminent power in the world today. When this belief is challenged by terrorism within US territory, or against US interests abroad, the faith in America's overwhelming might and ability to protect its citizens is damaged.[79] As discussed in chapter 3, the proactive strategy of counter terrorism can significantly decrease the risk of terrorist attacks and thus decreases the cost, which would otherwise occur, to the government's reputation.[80]

The costs to reputation when analyzing the effects of crime are not as predominant as that of terrorism. This casual attitude toward crime's detrimental effects is once again attributable to the incredible frequency of its occurrence. Americans simply accept that crime runs rampant among its streets. In addition, much of the crime is either not reported, is unknown, or is simply unobserved. Thus under the current strategy the government's reputation for dealing with crime is already extremely low.[81]Through the proactive strategy, with IO in the forefront, this reputation can be rebuilt through more

[78] The ineffective and random submarine-based attacks on the West coast during WW II are deemed to be insignificant. In addition, Hawaii at the time of the attack on Pearl Harbor was not a state, but a US-held territory.

[79] 46% of Americans believe that the government is not capable of preventing future terrorist attacks, The Gallup Poll 1995, The Gallup Organization Interview date: 4/20/95, survey # GO 22-50001-019

[80] The concept of government reputation is presented in Jonathan Mercer, *Reputation and International Politics,* (Ithaca NY: Cornell University Press, 1996)

[81] The percentage of Americans who feel that crime is the country's largest problem has grown from 4% in 1978(interview:2/10-13/78, survey # 993-k) to over 25% in 1997(interview date: 1/10-13/97, survey # GO 116007). Over 50 % of Americans fear going out on the streets by themselves after dark. The Gallup poll 1997(same survey), The Gallup Organization.

effective counter efforts that keep international crime out of the US. This will bring back the streets to the American people and eliminate a significant barrier to their success.

At the international level the US government's reputation is also affected by its ability to effectively combat both terrorism and crime.[82] An increased effectiveness in these endeavors and the subsequent adjustment in reputation tend to serve two major purposes. First, a reputation in which the US takes an effective approach to terrorism and crime will imbue confidence in foreign cooperation, both politically and within the commercial sector. The second effect of a proactive strategy will be to deter the terrorist and criminal organizations, as well as the foreign countries that support them. This enhanced US reputation might reduce the need to conduct coercive diplomacy

Reputation is not only affected by how effective the US is at combating terrorism and crime, but also by the methods employed to reach this effectiveness. This issue delves into the areas of "just warfare" and "waging war justly." When dealing with non-state actors like terrorists and TCOs, many of the concepts in both these areas seem to be fairly clear. The concepts initially developed by Thomas Aquinas and further developed to encompass information operations by John Arquilla, are now further refined to focus on the use of a IO led proactive strategy when dealing with terrorism and TCOs.[83]

The three concepts encompassed within a just war are: right purpose, duly constituted authority and last resort. As described by Arquilla, these concepts seem to be tested and strained when applied to IO. However, when IO is incorporated against both terrorists and TCOs, these concepts fall nicely into place and support the conduct of IO against these groups as both ethical and just. The continuing criminal activities as well as

[82] Jonathan Mercer, *Reputation in International Politics,* (Princeton: 1996)
[83] See footnote 77 above

the ever-present terrorist threat that assaults the US on a daily basis, provides all the justification necessary to sell the concept of self defense. If this were not enough, the concepts of preserving the "American way of life" in which all persons are promised the noble rights of life, liberty and the pursuit of happiness, renders more than adequate arguments that these operations are being performed for the "right purpose."

The concept of duly constituted authority provides the US with a double victory. While the government unquestionably possesses the traditional concepts of authority, the terrorists and TCOs do not. The last concept of "just war" that perhaps requires greater scrutiny when incorporating IO, is that of last resort. However, once again the conventional concept of last resort is significantly different when dealing with non-state actors. The traditional concepts of negotiations, treaties, and "deals" in an effort to resolve a conflict are inappropriate. These organizations have in the past and will continue in the future to conduct unlawful acts that either directly or indirectly result in death, destruction, and disruption. There is no other option when dealing with these groups. Thus, while performance of information operations may incur a significant cost to reputation when dealing with legitimate state actors, it is seen that these same costs are virtually non existent when dealing with terrorists and TCOs.

When analyzing the concepts of "just warfighting" the costs are once again minute. The concepts that encompass "just warfighting" include; noncombatant immunity, proportionality and striving to do more good than harm. In the case of noncombatant immunity, the target focus that IO can provide virtually eliminates this issue as a concern. IO directed specifically at terrorists and TCOs avoids this dilemma. Because these groups are non-state actors, the US can target them without affecting the

civilian population in which they are located. In this respect, IO becomes more ethically acceptable than conventional forms of warfare. When directed against a state sponsor of terrorism, a properly executed and focused IO attack can reduce or escalate the amount of collateral effects felt by the noncombatant population. In addition, it is more likely that an appropriately delivered threat of IO attacks (overtly or suggested) will provide the necessary coercive incentive to abandon their support for terror or crime.

At first glance, the concept of proportionality looks like it may be difficult to achieve. However, when placed in context with the fact that the concepts behind terrorism and crime are aimed at the complete collapse of US society and prosperity, then one can say that "the gloves are off." In addition, the ultimate concept behind using IO against terrorism and crime is the complete collapse of these groups. Thus, proportionality is a non-issue in this case. Finally, the concept that IO utilized under these circumstances should do more good than harm is self-evident. The danger in fulfilling this criterion is seen from the risk of legitimizing this form of warfare and setting a precedent, as discussed below.

Degradation of the government's reputation has the potential to cause significant problems, both domestically and in the international community. Domestically, these problems can take the shape of significant civil unrest. Internationally, a maligned reputation can have implications for treaties, commerce, alliances and global influence. As terrorism and transnational crime increase in size and scope, the manner and effectiveness of the government's ability to combat these threats will play a large role in determining its own reputation. The proactive approach to countering terrorism and crime provides the ability not only to maintain, but to enhance this reputation.

D. PRECEDENT

The government sets a "precedent" whenever it incorporates a new strategy or performs any untraditional action. This precedent can have serious repercussions on a government's reputation, as discussed above, and is discussed in greater focus here. In addition to affecting reputation, the setting of a precedent brings about several other issues that must be addressed. These issues include the potential for legitimizing the new action to the rest of the world, and the risk that the action may be conducted inappropriately and inefficiently.

When the government starts to perform operations that are traditionally uncharacteristic in any significant form, it changes the "rules" by which the rest of the world believes they are playing. This changing of the rules creates some positive and negative effects. By conducting business in a "new" manner, the government is sending out a message that it is unhappy or unable to deal appropriately with the current situation by usual means. Assuming the government is conducting business in the best interest of the country, this new action is an attempt to resolve the problem more effectively. In the case of the US and the problem of terrorism, the Tomahawk missile strikes on Osama Bin Laden's terrorist network, although reactive in nature, were unprecedented actions against international terrorism. These strikes not only raised world consciousness, but also pronounced US resolve and stand as a warning to deter others. While this new precedent in US counter terrorist efforts sent out a strong message to the world, it also showed, in this particular case, US disregard for world opinion. While the US may care very little about diplomatic ties with a country like Sudan, US reputation with its

European allies and many others is quite important. This situation raises the significant issue of, to what extent if any the US should include its allies in determining the implementation of a new counter terrorism and crime strategy.

The issue of how the US should treat foreign allies when determining an appropriate counter terrorist and counter crime strategy is best described as diplomatic cost, and is broken up into three issues. First, to what degree if any should these governments be informed of our strategy? Second, should these countries be invited to cooperate in formulating and executing this strategy? Third, to what degree should their opinion influence US decisions? These three issues are critical in a discussion on cost and become even more so when dealing with the potential use of IO in a proactive strategy.

One of the key aspects in US current reactive strategy towards terrorism is the reliance upon international cooperation. This cooperation is critical in developing administrative measures used in counter terror and crime as discussed previously. However, when addressing the proposed proactive strategy, international cooperation or lack of it, has the potential to be very costly. Under the proactive strategy, international cooperation will remain in place for administrative matters. However, foreign inclusion in the IO realm has many dangers. The use of IO is a controversial matter within the US government itself. When the concept is brought into the international arena, the divisions become wider. Many foreign governments may find the intrusive ability of IO a very troubling matter, and while allies do not "spy" on each other, the knowledge that IO can be conducted in an extremely covert manner may cause international discomfort. Perhaps the most significant cost in sharing US intentions to utilize IO, is the possibility that the information will be leaked to unwanted parties. This will allow these parties either to

prepare for this strategy by creating counter measures or, as discussed below, to preempt the US with their own IO attacks. By not involving allied governments into the strategy implementation process, the US government risks a significant outcry of protest, and potential alienation from allies.

Another extremely important issue that can potentially create significant cost is the danger that the US's use of IO could encourage a more permissive view of IO as an accepted form of warfare. Over the past decade the US has developed an enormous information and communications based infrastructure. This infrastructure is significantly larger than that of any other society. Because of the extent to which the US relies upon these systems, any attack that targets this infrastructure could be devastating.[84] In other states, which rely less upon information systems, the damage would be relatively less severe. Thus, while the US may have greater IO capability, the US could very easily "lose" in an exchange of IO attacks. This fact becomes increasingly relevant when dealing with non-state actors such as terrorists and criminal organizations. For these reasons alone, the cost of conducting IO would seem to be exceptionally large. However, the very nature of terrorism and crime may make this aspect of cost immaterial. Terrorists and criminals will inherently utilize any method available to fulfill their objectives. This includes the use of IO techniques. This is precisely why the US must act now. Terrorists and criminals are quickly enhancing their capability to strike the US via the huge information and communications networks and they will employ these IO tactics regardless of US action.

[84] A good discussion on the threats and potential consequences of cyberwar is found in Richard Hundley and Robert Anderson, "Emerging Challenge: Security and Safety in Cyberspace," *IEEE Technology and Society*, (Winter 1995/1996), pp. 19-28

Where the cost of setting a precedent may more likely be incurred is within the legitimate state system. The danger of utilizing IO, even against non-state actors, is that foreign states may see this employment as an opportunity to justify their own use of IO against the US, or another state. This danger becomes greater if the US use of IO is aimed at disrupting or destroying a state's terrorist support structure. While the goal of the operation may be to eliminate the terrorist organization, the support structure itself is a state function. These states may feel justified in conducting what they deem as retaliatory IO attacks on the US. While this danger legitimately exists, there are several factors which tend to mitigate this cost. IO techniques have the ability, if performed appropriately, to remain unnoticed or to confuse the situation to an extent that tracking the cause of "the problem" is difficult and ambiguous. As mentioned previously, the simple threat of aggressive IO attacks, either overtly or suggested, may be sufficient to convince foreign states to refrain from not only the support operations, but also from considering retaliatory IO attacks. In addition, an overt threat of conventional massive retaliation to any IO attack targeting US interests may cause foreign states to reconsider their actions. The remaining factor that reduces the risk of a hostile state's use of IO against the US are the currently in place administrative and diplomatic measures.

Another cost, which best fits under the precedent heading, is that of "wasting the asset."[85] This cost is incurred if, after the initial use of IO, factors are applied which render additional use either unacceptable or ineffective. The factors, which would render the continued use of IO unacceptable, include the potential outcry from world opinion

[85] In the introduction of *From Troy to Entebbe; Special Operations in Ancient and Modern Times*, (University Press of America, 1996), John Arquilla defines "wasting asset"; "(that which) works well the first time because of its novelty may soon lose its luster as familiarity and the development of countermeasures improve the defenders' chances."

and the potential threat of reciprocal IO attacks. If the international community gained the knowledge that the US had utilized IO, even against non-state actors, the potential for significant protest and the push for administrative punishment may exist. As mentioned previously, the use of IO-based attack is a very controversial issue in the world community. The notion that the US had disregarded these concerns for its own benefit, and without consultation with others, might anger many states. This anger might even culminate with the threat from foreign states to implement reciprocal IO operations. The extent of this external pressure may be sufficient to abandon the use of IO in future action.

Another reason that an IO-based attack may become a wasted asset, is the potential for the target organizations to adapt and innovate around these attacks and virtually render further IO operations ineffective. Once the use of IO-based attacks are observed by these organizations, counter efforts will be performed. These efforts include the building of secure systems that would significantly upgrade integrity, or simply innovating around their use.

On the domestic side, the political opposition to IO-based operations may prove sufficient to relegate its conduct to a "one shot deal." The factors that would most greatly affect the opinion of domestic policy makers would be the effectiveness and appropriateness of the initial attack. If operations were conducted that were unobserved by outside parties and were seen to provide a significant victory against terror or crime, the IO-based attacks might be allowed to continue, at least till the first mishap. If, on the other hand, a mishap were to occur, the parties in opposition to this form of tactic would "scream bloody murder," and make a significant effort to eliminate its use.

In this section, several costs have been lumped together under the heading of "precedent." All these costs relate, to varying degrees, to the initial use of IO- based operations. While many of these costs are potentially great, they are mitigated by two key issues. First, if performed properly, many of these costs are non-existent; and second, the potential benefit of these operations likely outweighs their cost by far.

E. ESCALATION

A danger in conducting any operations against terrorists, whether proactive or reactive, conventional or IO, is the risk that the terrorists will escalate the conflict. In order to understand the degree of risk it is necessary to understand why this escalation may be performed, and how it is affected by counter efforts. Two basic reasons stand out as the main cause of escalation. These are retaliation and losing ground. Terrorists are very conscious of their image, in both world opinion and within their own constituencies. In order to maintain constituency support and gain world respect, they must present themselves as strong and resilient. Thus, when a terrorist organization is attacked, it must respond to this attack or risk losing credibility. The magnitude of the response must be sufficient to provide the illusion that the organization was not significantly damaged and that they are capable of not only retaliating but doing so with greater power.

Another reason why terrorists may escalate the conflict is simply because they feel that they are losing ground in obtaining their goals. This point is amplified if the terrorists feel that their organization is on its "last legs." In an effort to revitalize the organization the terrorists may feel that a significant act, that would warrant considerable

attention from the media and the world, is their last hope. As death and destruction become an ever-present aspect of everyday life, this escalation may end up being significant, to include the use of WMDs.[86]

The proposed proactive IO strategy has the potential both to inflame as well as to extinguish this cost. In many cases, retaliatory strikes are conducted to maintain or enhance one's reputation. Thus when an attack is performed overtly by conventional means as was seen with the Tomahawk missile strikes in August 1998, the threat of retaliation is considerable. However, if an attack on a terrorist organization were conducted covertly, two important factors would arise. The humiliation absorbed by the terrorist organization would only be a fraction, compared to what it would suffer from an overt attack. The absence of media attention that would be associated with this low to zero profile attack would thus alleviate the need for the terrorists to conduct operations in an attempt to "save face." The second factor of a covert operation would simply be the inability of the terrorist organization to determine who performed the attack, if they were able to deduce that an attack was performed at all. In addition, by either entering into their decision process or destroying this decision process, the US would be able to disrupt their planning cycle. By hampering the group's ability to properly organize, the US can effectively reduce the prospects of a retaliatory strike.

The nature of current US counter terrorist strategy is to slowly wear away the capabilities of terrorist organizations until they become too weak to operate successfully. If indeed this strategy was effective, it would, at some point bring the terrorists to a point

[86] Jerold M. Post in his article "Prospects for Nuclear Terrorism: Psychological Motivations and Constraints," *Preventing Nuclear Terrorism,* ed. Paul Leventhal and Yonah Alexander, (Lexington MA: Lexington Books,1987), pp. 101, discusses the potential for "terrorist losers" in an attempt to "regain prominence" may resort to nuclear weapons.

of desperation. It is at this point that the risk of a highly escalated attack would occur. The proactive strategy avoids this threat by providing the possibility to seriously weaken a terrorist organization in a limited amount of time. In addition, the proactive strategy keeps the terrorists on the defensive and subsequently prevents the terrorists from sustaining and introducing new operations. As discussed in a previous section, the threat of terrorist organizations escalating into IO-based attacks, while present, is irrelevant to this analysis. The terrorists will utilize this weapon regardless of US actions.

In the case of criminal escalation, the danger is from the criminal's increased violence and accelerated progression toward terrorist tactics. The incorporation of the proactive strategy will substantially increase the effectiveness of counter crime efforts. Yet this effectiveness might for the first time make a relevant impact on criminal activity. Placed in this unfamiliar situation the criminal may be inclined to seek new ways of doing business. This may include the conduct of operations that are inherently more risky, branching out into new untapped markets, or increasing levels of violence. This increased violence could come in one of two forms. The first, would be increased violence between rival criminal organizations. As the proactive strategy decreases both supply and demand, the criminal organizations might begin to fight amongst themselves in order to gain control of limited resources and market share. This would include both the domestic gangs, in which rival violence already occurs, but also the cartels and major organizations themselves. This inner fighting has both a positive and negative effect. The rivalry to some degree will perform the task of eliminating a percentage of the criminal organizations, or at least some of the people that are employed within these organizations. The negative effect is that this violence may very well spill over onto the

streets where innocent people will inevitably get injured. The second form of violence is perhaps the more alarming. This violence consists of increased use of terrorist techniques in the attempt either to intimidate police and government officials into ceasing their prosecution, or simply to wage a form of warfare against the authorities that are impeding their progress.

F. FOREIGN SOVEREIGNTY

Foreign sovereignty must be considered whenever the US conducts operations outside of its own territory. The potential costs of violating sovereignty are significant and range from world condemnation, retaliation, and a damaged reputation. When dealing with non-state actors such as terrorists and criminals, the issues behind foreign sovereignty become clouded; and when the concept of IO is included they become even more ambiguous.

As is being currently seen with the decision to intervene in Kosovo, any determination to violate sovereign territory is a very difficult and closely scrutinized matter. Consensus with other states is normally a key factor in forming this type of decision. Ignoring world opinion by conducting unilateral action, as discussed earlier, has the potential to create enormous world criticism. Much of the international community's concern behind any violation of sovereignty, is the fear that by not advocating every state's right to sovereignty, their own may some day be ignored.

Perhaps the greatest danger in violating sovereignty is the potential for the state that was violated to seek retribution. This retribution can come in many various forms. The most acceptable, in the eyes of the US, would be purely administrative measures,

including sanctions, diplomatic isolation etc. There are three reasons why this will most likely not be the form of retribution. First, the US itself did not utilize administrative measures so why should they? Second, administrative measures will only be effective if they gain support of the world community, which the US leads. Third, the state seeking retribution was already conducting some action that was deemed atrocious or unlawful, so they are probably not constrained by morals.

The more likely and more disconcerting form of retribution is in the form of some level of violence. This violence can take the shape of limited strikes (which will inevitably be labeled terrorism by the US), or all out war. The probability that a foreign state will initiate a conventional war with the US is minute. The conventional capability of the US military would make pursuing this course suicide. Thus the state is in all practicality limited to terrorist-type attacks.

All international terrorist and criminal organizations utilize the foreign sovereignty issue as a shield against US "persecution." Some of these organizations do so with the knowledge and support, either active or passive, of the "host" country. Others do so by taking advantage of a state's weakness and inability to prevent it. Sovereignty is defined as authority in and control over an area. Thus an argument can be made that states that do not have the ability to prevent terrorist and criminal organizations from operating within their territory, do not actually possess sovereignty anyway. While this may actually be a very good argument in the academic realm, it has little application in world politics, where its practical application is unrealistic. Thus, any conventional method used to attack these organizations must pass into and intrude upon foreign soil and, to some degree, violate another country's sovereignty.

The use of IO has the potential to eliminate the requirement for any physical incursion into foreign territory. While this lack of physical presence greatly reduces the cost of sovereignty violation, it does not necessarily eliminate it completely. The concepts behind cyberspace incursion are not as of yet fully developed. None the less, the advent of IO within a proactive counter terrorist and crime strategy provides numerous advantages that can greatly reduce the costs associated with violation of foreign sovereignty.

First, there are no clear international laws that govern the use of information operations.[87] While many countries are struggling to obtain a clear understanding of its implications, others are ignorant of its capabilities. In fact, research and continued innovation are being performed every day that transforms IO capabilities and subsequently alters the likely repercussions from its use. In addition, IO can be conducted with extreme subtlety. Unlike Tomahawk missiles, which provide enormous visual evidence of use, IO can be accomplished without detection. The claim that sovereignty was violated is quite obvious with conventional methods; however, with IO, such violations are extremely difficult to prove. In addition, IO allows the US to target the information and communications systems of terrorists or criminals specifically. These systems are the personal property of the organization and not likely of the government of the state where they are located. By solely attacking these systems and avoiding any damage, or for that matter avoiding the need even to touch foreign soil, it becomes extremely difficult for states to claim that a violation of sovereignty has occurred.

[87] A good discussion on the threat of cybercrime and the lack of sufficient international law is provided in Louise Shelley's article "Crime, Corruption and Technology in a World Without Borders," *Journal of International Affairs*, Spring 1998, Vol. 51, No. 2, pp. 605- 620

Terrorists and criminals have long thrived behind the shield of foreign sovereignty. They conduct their operations with relative impunity, running back to hide when necessary. IO provides the US with a tool that can reach these organizations. While not totally eliminating the cost of sovereignty, IO significantly reduces it.

G. CIVIL LIBERTIES

Civil liberties are among the most closely guarded rights in the US. The concept of civil liberties is derived from the first 10 amendments of the Constitution known as the "Bill of Rights," and is intended to prevent the abuse of the government's power. When discussing the conduct of IO, the two amendments most feared to be in jeopardy are the First, which guarantees free speech, religion and press, and the Fourth, which protects against illegal search and seizure. Any discussion that includes the possibility of infringing upon these rights, regardless of how minute, is highly scrutinized and is virtually political suicide. The fear that "big brother" is watching is enough to send civil rights advocates scrambling into action. The protection of these rights tends to be viewed by some as an absolute, without regard for the consequences.

While some advocates would claim that these rights must be held above all others, even Supreme Court Justice Oliver Wendell Holmes stated that this freedom must stop at "shouting 'fire' in a crowded theater." Clearly, there are situations in which the greater good of the community must prevail over individual rights. The growing threat of more powerful terrorist attacks, as well as the ever increasing assaults from criminal activities pose key dilemmas. The appropriate and supervised use of IO does not impinge upon the rights of law-abiding citizens, but rather is designed to ensure these rights for future

generations. It must also be brought out that, in the domestic realm, the use of IO would only be necessary in a very limited number of cases, and would be implemented only after proper authorization was received. The overwhelming majority of US citizens (well over 99%) would suffer absolutely no effects from the use of IO.

While performing IO operations is in the interest of preserving the freedom which US citizens have become accustomed to, the potential for significant public outcry exists.[88] While the knowledge of IO within the proactive strategy must, for previously stated reasons, be a very sensitive and restricted matter, this secrecy may itself cause turmoil. The knowledge that IO is being undertaken by the government will inevitably become known to the public sector. The fear that these operations will infringe upon the rights of ordinary citizens, or will be utilized for political purposes, might cause public outcry and a demand for its termination. Properly preparing for these accusations may help to mitigate these costs. If necessary, providing the facts about IO could educate the public to its effectiveness and exceptional discrimination. In addition, appropriate checks and balances that relegate it use and ensure its appropriateness, will diminish the fear of unwarranted intrusion into the public realm.

When analyzing the cost to civil liberties, it is necessary to address the costs that are currently incurred under the existing reactive strategy. The American people have already incurred a cost on their freedom. This cost is seen in the fear of walking the streets at night, or the fear that their son or daughter might start using illegal drugs. It is also seen when businessmen are unable to provide for their family because they were

[88] The percentage of Americans who would accept increased surveillance upon US citizens rose from 37% in 1995 (interview: 4/20/95, survey # 22-50001-019) to over 45% in 1996 (interview: 7/29/96, survey 107357). When asked the same question with regards to foreign citizens residing within the US, 63% of Americans favored increased surveillance practices. Gallup Poll, 1996, The Gallup Organization.

driven out of business or robbed by organized crime. Even more devastating is the cost associated with the loss life from a terrorist bomb. Virtually all the previous cost factors discussed above play a role in determining an individual's civil liberties and rights. The accumulation of these costs will become increasingly clear in the cost comparison provided below.

H. COST COMPARISON

Seven separate cost factors associated with counter crime and terror have been analyzed. These cost factors can be combined into an "aggregate cost." The factors are not valued in numerical terms, but rather relatively. Thus, the comparison that follows is a measure of relative rather than absolute values. In addition, each of the costs are probabilistic in nature and are based on past experience and an assumed proficiency in IO-based operations. The methods to achieve this proficiency will be discussed in chapter 5.

Under the current reactive strategy, the US has experienced an average of 90 terrorist incidents per year.[89] The aggregate cost inflicted by each incident is a reflection of the severity or intensity of that particular attack. Intensity is the term utilized to describe the potential death and destruction inflicted by a single specific attack. As a general rule of thumb, as the intensity of a terrorist attack increases the value of each of the seven cost factors will increase. As the cost factors increase the aggregate cost of that attack rises correspondingly.

[89] Terrorist incidents directed at the US or its interests abroad. Based on 5 years 1993-1997, *Patterns of Global Terrorism*

Figure1 below provides a visual representation of aggregate cost associated with various types of terrorist attacks. While the actual realized cost of any attack will be determined by the specific details, this diagram provides a general representation. The curve begins with the aggregate cost associated with an individual shooting. This incident assumes an average, non-politically significant individual who is targeted for the simple fact that he or she is an American. At the other end of the spectrum is the increasingly plausible scenario of a terrorist use of WMDs. Spanning virtually the entire range is the cost associated with cyberterror. Cyberterror is able to encompass the full cost spectrum due to its inherent ability both to focus on a very specific target, or to be very indiscriminate and broad. It must be noted that the most severe attack observed during the past 10 years has been the New York World Trade Center bombing, yet when plotted on the attack intensity curve this attack is at the midrange of the spectrum.

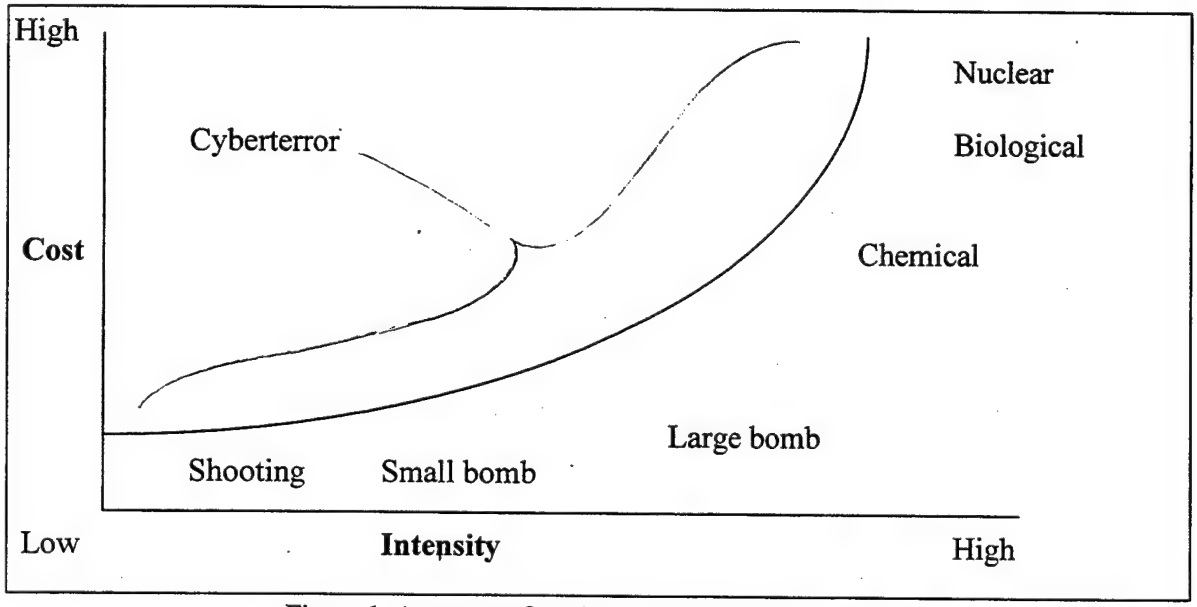

Figure 1: Aggregate Cost for Terrorist Attack Intensity

As each attack is performed the total cost increases accordingly, and at the end of the year, (or any designated time period) the total cost is derived by summing all the individual aggregate costs. Thus in an average year where 90 terrorist attacks are performed, the total cost incurred due to the employment of the reactive strategy is quite large.

The proposed proactive strategy invokes a cost prior to the conduct of any terrorist act. This initial cost, absent under the reactive strategy, is representative of the expense associated with the use of IO. The preponderance of this initial aggregate cost is felt in terms of pressures imposed on civil liberties and foreign sovereignty.

Although complete success is not likely, the proactive strategy may be able to stop a large percentage of low intensity terrorist attacks. Thus, just as with the reactive strategy, total cost will be a summation of each incident's aggregate cost, but will include the above mentioned initial cost of IO. The IO-based proactive strategy will provide a significantly greater ability to prevent the greater intensity attacks, including WMD and cyberterror. This is true because the preparations for these attacks are of high profile and can be detected with the use of IO. The cost savings associated with preventing a WMD attack, by itself, justifies the incorporation of the IO-based proactive strategy. The questions that must be asked are how great a cost does the analyst believe utilizing IO engenders and how many terrorists attacks or how intense must an attack be before this cost is deemed acceptable?

The sheer number of transnational criminal acts conducted on a daily basis renders the valuation of aggregate cost for each incident intangible. Crime is a perpetual

problem that must be viewed in larger overall terms. Thus the total cost, which as with terrorism is the sum of aggregate costs, will be the focus of this analysis.

The current reactive strategy towards crime has allowed criminal organizations to expand their illegal operations, enter into profitable cooperation agreements, and even enter into the legitimate business world through illegitimate means. As the criminal world becomes increasingly "high tech," maintaining the reactive policy will continue to benefit the criminals and impose an increasing cost upon the American people. Thus the total cost of crime, already at a staggering level, is continually rising at an increasing rate.

As with terrorism, the proactive strategy toward crime brings with it some initial costs. The initial aggregate cost is a combination of the cost due to current crimes as well as the cost incurred from using IO. As the proactive strategy is incorporated, the total cost will decrease in proportion to the decrease in crime. Similar to the terrorist analysis, the proactive strategy's effectiveness will most likely be less than 100 percent. However, even if some crime continues, the aggregate cost will still decrease significantly and will ultimately stabilize at a certain level well below that of the costs imposed by the reactive strategy.

I. CONCLUSION

In order to justify accepting and implementing a proactive strategy in the US's battle against terrorism and crime, a clear benefit over the current reactive strategy has to be established. With this in mind, seven cost factors were analyzed in this chapter, to capture the costs involved with each strategy. The aggregate cost of each terrorist

incident is determined by summing the value of each cost factor. The total cost, of any time period, is thus the summation of the individual aggregate costs. The total cost of each strategy was then compared and the relative cost savings established.

Within both the cases of terror and crime the proactive strategy was seen to provide substantial cost savings. While the proactive strategy brings some inherent costs that are not present with the reactive strategy, the devaluation in other factors more than overrides these costs. While the value assigned to each of the cost factors will ultimately be determined by expert analysts, allowing perhaps some degree of bias, the cost comparison analysis maintains its importance and relevance. The proposed proactive strategy, which incorporates significant IO-based operations, provides the US with an instrument to combat terrorism and crime effectively at the lowest possible cost to the American citizen.

V. THE TOOLS AND WEAPONS

This chapter analyzes the application of advanced technologies under the proposed proactive strategy for countering terror and crime. A good starting point is provided by the notion that proactive information operations can be divided into two categories: the strategic and operational attack paradigms[90]. The strategic attack paradigm describes the use of information operations as a distinct weapon that can be used independently.[91] The operational attack paradigm uses information operations as a tool in support of other, more "conventional," means. The proactive strategy proposed herein employs both paradigms in its effort to counter terror and crime. When applied to terrorism and crime, the strategic attack paradigm is divided into three areas; intelligence collection, disruption and destruction. The performance of these three actions entails the use of advanced computer systems (predominantly in the realm of cyberspace), advanced weaponry and psychological operations. Under the operational attack paradigm, information operations are used to enhance reactive measures. In particular, the superior intelligence provided by information operations will significantly empower prosecution and administrative measures.

[90] Michael L. Brown, *The Revolution in Military Affairs: The Information Dimension,* (Fairfax, VA, AFCEA International Press, 1996)

[91] This concept is addressed by Roger Molander, Andrew Riddile and Peter Wilson, *Strategic Information Warfare: A New Face of War,* (Santa Monica, CA: RAND 1996).

A. INTELLIGENCE COLLECTION

Perhaps the greatest drawback of the proactive strategy is the heavy requirement for intelligence. This intelligence must be accurate, timely and both qualitatively and quantitatively sufficient to allow for the proper conduct of operations. However, the US intelligence community is currently ill-prepared to deal with the information savvy terrorist and criminal of the 21st century. Current intelligence assets were designed to cope with the Cold War threat, and while these assets are still being effectively utilized, they are neither appropriately focused nor adequate to cope with either terrorism or transnational crime. The products obtained from SIGINT, IMINT, and HUMINT are all limited, due to the principally non-state nature of terrorist and criminal organizations. As these groups accelerate their reliance upon advanced intelligence systems, these traditional collection methods will become increasingly antiquated. Scott D. Breckinridge writes:

> "The terrorist world is an extremely difficult intelligence target, the groups being small elusive and often unknown, even to those friendly to them. The security and intelligence forces charged with blocking their depredations are likely to meet more failure than success."[92]

Today's SIGINT capabilities derive primarily from intercepted of communications and radar emissions. However, terrorist and criminal organizations provide an extremely limited communications footprint. In addition, the communications that are performed are done through the use of encrypted digital cellular telephones and

networked encrypted computer systems. These technologies make it extremely difficult both to intercept and decrypt communications. While the US government has limited the ability of legitimate businesses to protect their computer systems, the availability of 128-bit DES encryption on the international market has provided terrorists and criminals the security they desire.[93]

IMINT has also displayed limited ability to gain the necessary information on terrorist and criminal activities. The overhead imagery provided by assets like the KH-15 spy satellite produce very little good intelligence on these threats. Perhaps the largest contribution is the occasional imagery of terrorist training sites and the location of illegal harvests for drug production. While this imagery may provide some useful information, computer programs are available that accurately calculate the time in which the satellites pass overhead. With this information, these organizations are able to mask their operations. The use of aircraft-based imagery from assets like the SR-71, U-2 or J-Stars is also quite limited. The costs and risks associated with violating sovereign airspace are also significant obstacles to their use for these purposes.

HUMINT is traditionally the most relied upon method used to provide relevant intelligence on terrorist and criminal groups. However, HUMINT has some severe limitations of its own[94]. The ability of intelligence agencies to plant an agent within these organizations is extremely limited. Members of terrorist organizations are often recruited

---

[92] Scott D. Breckinridge, "Intelligence after the Cold War," *International Journal of Intelligence and Counterintelligence,* Fall 1997

[93] A discussion of the encryption issue is presented in James Adams, *The Next World War,* (New York: Simon & Schuster, 1998), pp. 213-223 and Senator John Kerry, *The New War,* (New York: Simon and Schuster, 1997), pp. 126-132

from known families, and at a young age, often 8 or 9. In addition the requirement to conduct terrorist operations is necessary to advance to any significant position within the organization. This, coupled with the fact that terrorist organizations are becoming increasingly networked and compartmentalized, means that the knowledge possessed by one individual is often severely restricted. The ability to "turn" an existing terrorist member is equally difficult, due to the fanatic and unreliable nature of many terrorists. On the criminal side, family affiliation is also extremely important in gaining entry into the upper levels of the organization. Some criminal organizations, like the Colombian cartels, employ former intelligence officers who perform background checks on potential "business" associates in order to validate authenticity.[95] Clearly, alternative methods of intelligence collection and a new mind-set are required if the US is to confront and prevail in the battle against terror and crime. The advanced technologies of the 21st century provide the necessary tools to perform this intelligence operation.

The collection of intelligence through use of advanced technologies is divided into two categories. The first is performed through manipulation and exploitation of computer systems. The second is the direct collection of information by advanced sensors and photography.

The embrace of advanced computer systems by terror and crime organizations, while increasing their efficiency and effectiveness, have also exposed these groups to new threats of surveillance and intelligence collection. This intelligence is collected by

---

[94] A brief discussion of intelligence capabilities against terrorism can be found in John Arquilla, David Ronfelt and Michele Zanini, *Networks, Netwars and Information-Age Terrorism,* (Santa Monica: Rand, 1999, forthcoming)

[95] Kerry, *The New War,* pp. 76-79

entering the organization's computer network and gaining access to computer files[96]. This process can be conducted in numerous ways but the most prevalent are through the use of sniffer programs, and backdoors. James Adams describes a sniffer program as:

> "A program that attaches itself to a computer system and records the first 128 keystrokes of people gaining legitimate access. Within those 128 keystrokes would reside the password and log-in information for that account. The sniffer would then transmit those keystrokes back to the hacker, who would have all he needed to roam around the target system."[97]

Once access is gained to the system, the hacker has virtual free reign to access any information within the system. As terrorists and criminals increasingly rely upon computers to organize their operations, the amount of information available for counter efforts will increase accordingly. The ability to view an organization's payroll, financial status and support structure can all be highly exploited. Other information, including equipment purchases, memoranda discussing future operations, or even personal information and correspondence can all be capitalized upon.

The "backdoor" program requires future planning on the part of the intelligence agencies[98]. The backdoor is a program that is initially implanted within the computer system, even before it gets to the customer. Once the system is in place, the operator simply calls up the computer, activates the backdoor and gains entry without having to know the password. Thus, arrangements are made with the manufacturers of the computer

---

[96] "Afghanistan, Saudi Arabia: Editor's Journey to meet Bin-Laden Described," *London al-Quds Al-'Arabia,* 27 November 1996, p.4

[97] Adams, *The Next World War,* p. 193

systems to allow government access. This arrangement is very delicate, considering the manufacturer's reputational concerns. If denied this sort of admittance, access can still be accomplished by intercepting the shipment during delivery. Another difficulty with implanting a backdoor program is identifying the correct computer systems. Terrorist and crime organizations will normally utilize a series of "fronts" or "middle men" to disguise the ultimate destination. However, even if only a small percentage of backdoors are ever activated the return will have been worth the effort. In addition, backdoor access can grant the hacker a "systems manager" status. This status allows the ability to erase entry data, cover all actions, and maintain anonymity. This renders the hacker's activity virtually invisible, and mitigates the potential problem of retaliation, or of source "cut-off."

Perhaps the greatest practical difficulty of this collection method is gaining the expertise necessary to carrying it out. While the US government possesses some extremely intelligent individuals, civilians form the vast majority of those with advanced hacker skills. In many cases, these civilian "experts" are identified only after they have hacked into the government's computer systems and were subsequently apprehended. An attempt to convert these individuals into public employees is a risky prospect, and has significant potential to backfire.[99] Thus, the intelligence agencies must somehow attract talented individuals through appropriate incentives or develop their own in-house expertise.

---

[98] A discussion of the ability of computer oriented operations is presented in an article by Valeri Lorenzo, "Guarding against a new digital enemy," *Jane's Intelligence Review,* August 1, 1997. These hacker concept are also discussed in Adams, *The Next World War.*

[99] The story of Justin Petersen, who was employed by the FBI after his own arrest, is recounted in Adams, *The Next World War,* pp. 156-157

The second method of intelligence collection is through the use of advanced sensors and photography. The advent of MEMS, Micro Electronic-Mechanical Systems, UAVs, Unmanned Aerial Vehicles, and MAVs, Micro Air Vehicles will provide drastically increased opportunity for enhanced sensor and imagery effectiveness. The US Department of Defense has spent over three billion dollars on UAV research since 1979, and the Defense Advanced Research Project Agency (DARPA) is budgeted to spend another half billion by 2003.[100] Much of the research is intended to support the conventional ground force commander by delivering enemy order of battle information, providing a "God's eye View." This technology has been tested and proven effective.[101] The Israeli and American aircraft industries have developed the Pioneer UAV that flew over 1700 hours during the Gulf War. The Predator UAV, of the US Air Force 11th Reconnaissance Squadron has already logged more that 3,800 hours flying over Bosnia-Herzegovina.

The primary advantage to employing UAVs is the lack of personnel required to enter potentially hostile territory. In addition, the UAV has significantly greater maneuver capabilities than manned aircraft, and presents a considerably decreased radar signature. A UAV utilizing noise-reduced propulsion can go completely unnoticed.

While the UAV has already proven to be effective, it is constrained by several factors. Among the greatest drawbacks is lack of endurance. Addressing this and other issues, DARPA has budgeted funds for projects like the Airborne Communications Node

[100]An in depth analysis of the current and future capabilities of UAV technology is presented in "Drone Wars," *Jane's Defense Weekly,* June 3 1998 and "DARPA UAV Technology Budgets top $500 Million," *Military Robotics,* , April 17, 1998

[101] "Drone Wars," *Janes Defense Weekly,* June 3, 1998

(ACN), which will provide extended range and rapid deployment of advanced military communications system. Programs like the Adaptive Spectral Reconnaissance Program will develop advanced reconnaissance systems based on spectrally adaptive imaging sensors. Another of the more promising sensing systems is the Millimeter Wave Targeting & Imaging System (MMWTIS). "This system will use active and passive techniques to achieve high resolution targeting and imaging"[102] at millimeter wave (W-band) frequencies. Once operational, these systems will provide an enormous amount of data back to the analysts. The volume of data itself presents a significant problem that is being addressed through programs like TRW's Applique.[103] This "system of systems" will compile data from all sources and provide the warfighter with a clear understanding of the battlefield.

When exploring the use of UAVs in the fight against terror and crime, an important development is the capability for intermediate platform control and automatic target recognition.[104] With the majority of terrorist and criminal organizations being located in remote or foreign territory, the US will not likely have conventional forces staged nearby. However, with intermediate platform control relay units, special forces can gain control of the vehicle and bounce imagery and information back to the rear. Another important development is the Unmanned Combat Air Vehicle (UCAV). These specially configured UAVs will be able to identify a target and deploy weapons systems. This capability along with the disruptive and destructive weapon systems, mentioned below, will be able to pay huge dividends in the fight against terror and crime.

---

[102] Jerome Chandler, "Microplanes; tiny spy planes," *Popular science,* January 1998
[103] Adams, *The Next World War,* pp. 111-115

While the UAV's sensors may be able to provide exceptional information, the limited endurance hinders the ability to maintain continues surveillance, so necessary to gaining specific information about terrorist and criminal operations. However, with a little ingenuity and the exploitation of MAVs and MEMS, this surveillance can be possible. Employing a UAV that can store these tiny technologies, fly to the target area, land and deploy these systems posses seemingly limitless possibilities. The use of special forces to deploy these mini systems is another potential employment tactic.

Professor Chih Ming Ho from UCLA has revolutionized the area of miniaturization. Chih's work in the area of avionics has propelled a new class of micro-sized sensing and mechanical systems, known as (MEMS).[105] As this technology is pursued, the capabilities of intelligence gathering will blossom. These MEMS will have the capability to carry a multitude of sensing devices able to detect motion, light, sound, smell, images and much more. The ability and size of these sensors have spurred concepts like ant spies, sensor grass, and surveillance dust.

MEMS have also spawned the development of Micro Air Vehicles (MAVs)[106]. MAVs are intended to be small enough to fit into the palm of the hand. Current development requirements call for a range capability of up to 10 km, speeds up to 30 miles per hour and mission duration times of 20 minutes to 2 hours. The operating time constraint is primarily due to the power expended during flight. If these systems were to land, or attach themselves to a host object, then the power can then be utilized by the

---

[104] The technology concepts are discussed in the articles referenced in footnote 11

[105] MEMS is discussed in Adams, *The Next World War,* pp. 122-137

[106] A good discussion on the capabilities and future of micro sized flying machines is presented by Jerome Chandler, "Microplanes; tiny spy planes," *Popular Science,* January 1998 and "DARPA UAV Technology," *Military Robotics,* April 17, 1998

embarked sensing equipment and significantly extend the operating life. In addition, research is currently being conducted on alternative propulsion systems that would extent the operating life cycle. This research includes concepts like a reciprocating chemical muscle (RCM) pioneered by Georgia Tech Research Institute, and the hydrogen-powered jet turbine from MIT.[107]

The military has pursued this technology as part of their "Land Warrior"[108] program. The concept behind Land Warrior is to provide the average infantry soldier a stand-off capability. In other words, the soldier of the 21st century will be able to launch MAVs from his rucksack and send them over the hill or around the corner, to determine enemy positions. When used in conjunction with UAVs or special operations forces these technologies will provide surveillance capabilities from extended ranges. In addition, as the size of high-energy weapons continues to reduce their employment by a Micro Combat Air Vehicle (MCAV) will become possible.

B. DISRUPTIVE & DESTRUCTIVE OPERATIONS

While gaining information is an extremely important function of efforts to counter terror and crime, it is normally collected in support of direct or indirect action. With the use of IO, this action can be predominantly non-lethal in nature, dividing into two categories: disruption and destruction. Often the difference will be simply the extent to which the IO tactics are employed. As an example, hacking into an airfield control system

[107] Chandler, "Microplanes; tiny spy planes," *Popular Science,* p.57
[108] Adams, *The Next World War,* pp. 109-120

can be performed simply to disrupt traffic, or it can be manipulated to cause a collision. These two categories can themselves be divided into three subsets: operations performed within cyberspace; operations utilizing advanced weaponry; and psychological operations.

When discussing disruptive and destructive operations in cyberspace, access to the terrorist or criminal organization's computer systems must be accomplished. As described above, this entry is accomplished through the use of backdoors, sniffer programs or during the initial programming back in the manufacturing process. Once access is gained, the programmer can install computer malicious codes (CMC) such as, Trojan horses, logic bombs, and worm viruses.[109]

The logic bomb is placed within the computer system prior to delivery to the customer, or can be inserted by a hacker once the computer becomes connected with the Internet. The logic bomb lies dormant and hidden within the system until activated. The "bomb" can be activated by a number of methods. These methods include: programming of a pre-designated time; activation by the programmer via the Internet or electrical emitting device; or the program can be designed to activate upon the performance of a designated function. In other words, the "bomb" can be designed to activate when the user enters the Net, when a particular e-mail address is called up, or when virtually any other normally performed operation is undertaken. Once activated, the programs can perform a myriad of tasks including releasing a virus, overloading the system or re-addressing communications.

[109] See footnote 9 above

A Trojan horse is a similar CMC device, but is entered into the system hidden within another program. Thus, when the targeted terrorist or criminal downloads or runs a particular program into his system, he unwittingly inserts the Trojan horse along with it. Once inside, the capabilities are the same as with the logic bomb. The Worm Virus is a program that is designed to self-replicate. The objective of the worm virus is to sufficiently utilize the system's computing power so that other operations are impossible, thus overloading the capability of the processing system. Another nasty tool is the polymorphic virus that changes it appearance every time it infects a new program. This continual transformation makes it increasingly difficult both to locate and destroy. While these programs can be designed to destroy an organization's computer systems, a greater profit may come from manipulation, as was discussed in chapter 3.

Advanced weaponry has also opened the door to numerous options for combating terrorism and crime. Many of these developing advanced weapons systems fall under the heading of Non Lethal Weapons (NLW)[110]. However, if employed by untrained personnel, and under certain conditions, these weapons can most definitely kill. Research into these weapons systems has been focused principally on their use by domestic law enforcement and military humanitarian and peace keeping operations. Thus, the potential for these weapons to cause greater damage than desired has slowed their acceptance. However, when applied to the matter of terrorist and criminal organizations, the strict necessity to limit injury and avert death does not seem similarly inhibiting. Thus, with

[110] Excellent discussions on advanced weaponry, to include NLW, is found in Douglas Pasternak, "Wonder Weapons," *US News and World Report,* July 7 1997 and "Measure for Measure," *Jane's Defense Weekly,* June 24, 1998, and in Adams, *The Next World War,* pp. 138-155

very little refinement, these systems can be refocused on terror and transnational crime organizations.

One of the more promising weapon systems is in the area of electromagnetic pulse or high energy radio frequencies (HERF). When utilized within the microwave frequencies (.5 - 100 GHz range), these weapons have the ability to "fry" the circuits of any electronic system. In addition, these systems can effect the internal structure of the human body causing pain, burns, epileptic seizures, cardiac arrest and even death. As the technology advances the effective range and precision of the weapon will allow for greater flexibility in use. Currently, the size of these weapons is fairly large. Thus employment must be conducted from a relatively large platform like a vehicle. However, US intelligence has learned of a Russian- built HERF weapon of extremely small size. The Weapon was code named the "Beer Can"[111] and tests have proven its limited effectiveness within a range of 1 kilometer. As advances in miniaturization and direction capability are made, the potential to mount a HERF weapon on a UAV will exist. This combination allows operators to perform their attacks from greater stand-off distances, and with virtually complete anonymity. The terrorists or criminals may not only be unable to determine the cause of the problem, but even if they suspect the cause they would be unable to verify the identity of the attacker.

Additional possibilities lie in the low frequency bands of electromagnetic radiation. This area is specifically intended to effect personnel. These low frequencies effect the chemical makeup in the human brain, releasing chemicals like histamines. As these technologies become increasingly refined they will possess the ability to put

persons to sleep or cause instant flu-like symptoms. Again, the possibilities when used against terror and crime are enormous. By virtually knocking out an entire terrorist headquarters, the US could significantly disrupt operations. The subsequent confusion and fear would provide additional collateral benefits.

Acoustic weapons are another emerging capability that affects physical structures as well as the human body. At certain frequencies, well below the human hearing level, subsonic waves can be used to vibrate internal organs. This vibration creates vomiting, loss of balance control and numerous other nasty effects. Due to the current inability to channel the waves in a specific direction, the operator would be affected along with the intended targets. However, when employed from a platform like a UAV, this drawback becomes irrelevant.

Finally, non-tech measures such as psychological operations need to be included as part of IO. Both the traditional military and the US government have neglected psychological operations. This neglect is due to the belief that psyops is an unconventional method that produces slow, if any results. In addition, the performance of aggressive psyops is often strongly opposed by human rights activists and liberals who believe that its performance is somehow immoral. With terrorism and crime both being unconventional threats, the conduct of psyops is a clear fit. When analyzing the potential of utilizing psyops against terror and crime, it is necessary to expand its traditional role. In other words, psyops must not be looked upon as simply dropping flyers and playing American music in the hope that the target audience begins to view the world with US colored glasses. Instead, perhaps the most nefarious, evil person available should oversee

[111] Adams, *The Next World War,* p. 151

psyops against terrorists and criminals. The idea is not to have these entities change their attitudes, but simply to change their actions. While lying, disception, misinformation, threats, embarrassment, and many others are counter to the US definition of psyops as "truth projection," they provide excellent possibilities when focused on terror and crime.

While the conduct of psyops is many times low-tech in nature, the advanced technologies mentioned above allow psyops to become increasingly important and effective. The interception or creation of false communications and E-mail can create internal fighting or instigate competition, even hatred between rival organizations. Concepts as untraditional as telekinesis or hypnosis might also be explored and exploited. In conduct of these operations, the operator must remember that these organizations are actively engaged in destroying US society. Thus, virtually any action to prevent their continued operations can be sufficiently justified, as discussed in chapter 4. Psyops should therefore also be a tool of counter terrorist and crime operations, and the conduct of disruptive and destructive actions should be designed to support the larger strategic psyops campaign. When confronting these non-state actors, psyops transitions from "winning their hearts and minds" to destroying them.

C. CONCLUSION

Exceptionally sophisticated and proficient, terrorist and transnational crime organizations have become the threat of the future. Their embrace of advanced computer and communications systems has significantly enhanced their efficiency, while providing access to new, exceptionally potent weapons systems. Their traditional behavioral

constraints have been overcome by their excessive greed, hatred and self-righteousness. US policy for dealing with these groups has become dangerously antiquated. By following its long-standing reactive policy, the US government places the entire nation in jeopardy. Only by adopting an aggressive, proactive strategy can these threats be constrained. This strategy must incorporate the same technologies that have propelled these groups to such increased power. While implementation of the proactive strategy incurs an initial cost, the eventual savings are likely to be enormous. Today's advanced technology provides the US with the tools necessary to engage in and win the war against terror and crime. Policy makers must now display the moral fortitude to implement these appropriate and very necessary measures.

BIBLIOGRAPHY

Adams, J., *The Next World War,* (New York: Simon & Schuster, 1998).

Aldrich, R., *The International Legal Implications of Information Warfare,* (Colorado Springs: Institute for National Security Studies, 1996).

Arquilla, J., "Ethics and Information Warfare," National Defense Research Institute, 1999 forthcoming.

----------. *From Troy to Entebbe; Special Operations in Ancient and Modern Times,* University Press of America, 1996).

Arquilla, J., Ronfeldt, D., and Zanini, M., *Networks, Netwar, and Information-age Terrorism,* (Santa Monica: RAND, 1999 forthcoming).

Baugh. W., and Denning, D., "Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism," *Trends in Organized Crime,* Vol. 3, No.1, 1997.

Breckinridge, S., "Intelligence After the Cold War," *International Journal of Intelligence and Counterintelligence,* Fall 1997.

Brown, M., *The Revolution in Military Affairs: The Information Dimension,* (Fairfax, VA: AFCEA International Press, 1996).

Crenshaw, M., "How Terrorism Declines," *Terrorism and Political Violence,* , Vol. 3, No. 1, Spring 1991.

----------. " Decisions to Use Terrorism: Psychological Constraints on Instrumental Reasoning," *International Social Movement Research,* Vol. 4, 1992.

----------. "An Organizational Approach to the Analysis of Political Terrorism," *Orbis,* Vol. 29, No. 3, Fall 1985.

Deutch, J., "Terrorism: Think Again," *Foreign Policy,* March 1997.

Government Auditing Office report, "Combating Terrorism," Sep 1997.

_____. "DOD Antiterrorism Program," NSIAD-97-207

Hoffman, B., "Responding to Terrorism Across the Technological Spectrum," *Terrorism and Political Violence,* Vol. 6, No. 3, Autumn 1994.

House of Representatives, Hearing before Committee on International Relations, Oct 1, 1997.

Hundley, R., and Anderson, R., "Emerging Challenge: Security and Safety in Cyberspace," *IEEE Technology and Society,* (Winter 1995/1996).

Jenkins, B., "The Study of Terrorism: Definitional Problems," *Behavioral and Quantitative Perspectives On Terrorism,* ed. Alexander, y., and Gleason, J.

Kerry, J., *The New War,* (New York: Simon & Shuster, 1997).

Laqueur, W., "Postmodern Terrorism," *Foreign Affairs,* September/October 1996

Libicki, M., *What is Information Warfare,* (The Center for Advanced Concepts and Technology, 1995).

Medd, R., and Goldstein, F., "International Terrorism on the Eve of a New Millennium," *Studies in Conflict and Terrorism,* 20:281-316, 1997

Mercer, J., *Reputation and International Politics,* (Ithaca NY: Cornell University Press, 1996)

Molander, R., Riddile, A., and Wilson, P., *Strategic Information Warfare: A New Face of War,* (Santa Monica, CA: RAND 1996).

Nacos, B., *Terrorism & the Media,* (Columbia: 1994).

National Military Strategy, *Shape, Respond, Prepare now- A Military Strategy for a New Era*, CJCS, 1997.

Netanyahu, B., *Fighting Terrorism,* (New York: Farrar, Straus, Giroux, 1995).

Pexton, P., "Cohen Focuses Sights on Terrorism," *Navy Times,* Sep 22, 1997.

Post, J., "Prospects for Nuclear Terrorism: Psychological Motivations and Constraints," *Preventing Nuclear Terrorism,* ed. Leventhal, P., and Alexander, Y., (Lexington: Lexington Books, 1987).

----------. "Narcissism and the Charismatic Leader-follower Relationship," *Political Psychology,* Vol. 7, No. 4, 1986.

Rapoport, D., "Fear and Trembling: Terrorism in Three Religious Traditions," *The American Political Science Review,* September, 1984, Vol. 78, No. 3

----------. "Sacred Terror: A Contemporary Example from Islam," *Origins of Terrorism: Psychologies, Theologies, State of Mind,* ed. Reich, W. (New York: Woodrow Wilson International Center for Scholars and Cambridge University Press, 1990).

Shelly, L., "Crime and Corruption in the Digital Age," *Journal of International Affairs,* Spring 1998.

----------. "Crime, Corruption, and Technology in a world Without Borders," *Journal of International Affairs,* Vol. 51, No. 2, Spring 1998.

The White House, "The National Drug Control Strategy: 1997 Budget Summary," February 1997.

Thornton, T., "Terror as a Weapon of Political Agitation," *Internal War,* ed. Eckstein, H., (West Port: Greenwood Press, 1964).

Tucker, D., "Responding to Terrorism," *The Washington Quarterly,* Winter 1998.

United Nations International Drug Control Program, "Drugs and Development," No. 1, 1996.

US Department of Commerce, 117th edition, Economics & Statistics administration.

US Department of Justice, Federal Bureau of Investigation, "Crime in the United States, *Uniform Crime Report,* September 1997.

US Department of State, *Patterns of Global Terrorism-1997,*

US Congress, Committee on the Judiciary Subcommitte on Technology, Terrorism, and Government Information, "A Nation At Risk, President's Commission on Critical Infrastructure Protection," November 5, 1997.

Van Creveld, M., *The Transformation of war,* (New York: The Free Press, 1991).

Williams, P., "Transnational Criminal Organizations and National Security," *Survival,* Vol. 36, No. 1, Spring 1994

Wright, R., *Sacred Rage,* (New York: Simon & Shuster, 1986).

Zimmerman, T., and Cooperman, A., "The Russian Connection," *U.S. News and World Report,* 23 October, 1995.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd
   Monterey, CA 93943-5101

3. Dr. Maurice Weir 2
   Associate Provost for Instruction
   Code MA/We
   Naval Postgraduate School
   Monterey, CA 93943

4. Professor Gordon H. McCormick 1
   Code CC/Mc
   Naval Postgraduate School
   Monterey, CA 93943-5000

5. Professor Eric Jansen 1
   Code CC
   Naval Postgraduate School
   Monterey, CA 93943

6. The Honorable H. Allen Holmes 2
   Assistant Secretary of Defense for SO/LIC
   The Pentagon, RM 2E258
   Washington, DC 20301-2500

7. GEN Peter J. Schoomaker 1
   Commander in Chief
   U.S. Special Operations Command
   MacDill AFB, FL 33608-6001

8. LT GEN William Tangney 1
   Commander
   U.S. Army Special Operations Command
   Ft. Bragg, NC 28307-5000

9. RADM Thomas R. Richards 1
Commander
Naval Special Warfare Command
NAB Coronado
San Diego, CA 92155

10. Maj Gen Charles R. Holland 1
Commander
Air Force Special Operations Command
Hurlburt Field, FL 32544

11. MG Michael A. Canavan 1
Commander
Joint Special Operations Command
Ft. Bragg, NC 29307

12. Jennifer Duncan 1
Center for Special Operations
Code (CC/Jd)
Naval Postgraduate School
Monterey, CA 93943-5000

13. Library 1
Army War College
Carlisle Barracks, PA 17013

14. Library 1
Naval War College
Newport, RI 02840

15. Strategic Studies Group (SSG) 1
Naval War College
Newport, RI 02840

16. Department of Military Strategy 1
National War College (NWMS)
Ft. Leslie J. McNair
Washington, DC 20319-6111

17. U.S. Army Command and General Staff College 1
ATTN: Library
Ft. Leavenworth, KS 66027-6900

18. Library 1
Air War College
Maxwell AFB, AL 36112-6428

19. U.S. Military Academy 1
ATTN: Library
West Point, NY 10996

20. U.S. Naval Academy 1
ATTN: Library
Annapolis, MD 21412

21. Maraquat Memorial Library 1
U.S. Army John F. Kennedy Special Warfare Center
Rm. C287, Bldg. 3915
Ft. Bragg, NC 28307-5000

22. Commander 1
Naval Special Warfare Group One
NAB Coronado
San Diego, CA 92155

23. Commander 1
Naval Special Warfare Group Two
NAB Little Creek, VA 23521

24. Commander 1
Naval Special Warfare Center
NAB Coronado
San Diego, CA 92155

25. U.S. Special Operations Command 1
ATTN: Command Historian
MacDill AFB, FL 33608-6001

26. Commander 2
USJFKSWCS
Ft. Bragg, NC 28307-5000

27. Professor John Arquilla 3
Center for Special Operations
Code (CC/AR)
Naval Postgraduate School
Monterey, CA 93943-5000